Post-Quantum Cryptography (PQC) Solution Analysis Guide

May 2026

The Post-Quantum Cryptography Coalition (PQCC) is a community of technologists, researchers, and expert practitioners with a mission to drive progress toward broader understanding and public adoption of post-quantum cryptography (PQC) and associated National Institute of Standards and Technology (NIST) standards. The PQCC emphasizes classical cryptosystems with quantum-resilient security to enable information security in an era of cryptographically-relevant quantum computers.

The views, opinions and/or findings contained in this report are those of the PQCC Authors and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

Table of Contents

1 Introduction

As organizations integrate quantum-resilient products and services, they must be prepared to assess these solutions in the context of their own priorities. This Solution Analysis Guide is intended to help your organization evaluate Post-Quantum Cryptography (PQC) solutions.

It supports the Post Quantum Cryptography Coalition's (PQCC's) Post-Quantum Cryptography Roadmap[1] by operationalizing early quantum-resilient solution analysis activities within the broader Post-Quantum Cryptography migration lifecycle. This Guide identifies initial analysis criteria for PQC solutions and maps out a model for scoring them. The guide also includes sample questions for technical domains that may apply to a solution (Appendix A).

Rather than jumping immediately into compliance checklists, this Guide encourages establishing a better understanding of PQC solutions in terms of post-quantum risk, organizational priorities, anticipated impacts, and solution timelines. The intended outcome of this process is to help organizations make better-informed decisions about PQC solutions throughout their migration. This activity will also help to identify high-risk dependencies involving quantum-resilient solutions that affect long-lived or sensitive data. Analysis outcomes can be fed into processes for inventorying, risk prioritization, and procurement for cryptographic migration planning.

This Guide is intended to be a starting point and not a one-size-fits-all model. Your organization should tailor the components and processes described to conduct its own analysis, iterate over time, and align with applicable government or industry guidance or requirements.

1.1 Scope

This Guide establishes key focus areas for analysis but does not strictly define the criteria for scoring within those focus areas. While conducting their analysis, organizations should define the specific scoring criteria best aligned to their needs. Criteria provided in this Guide are examples derived from existing best practices (frameworks, maturity models, etc.). A solution provider may be an external vendor that your organization works with or is considering for procurement, or a capability management group within your own organization. The processes described in this Guide can be initiated during a standard vendor or capability assessment, as part of a risk assessment process, or as a dedicated PQC migration activity.

[1] https://pqcc.org/post-quantum-cryptography-migration-roadmap/

The Guide should be tailored not just to organizational concerns, but also to the technical solutions being evaluated. Solutions may be products (for example, software or hardware) or services provided by a vendor. Appendix A details evaluation considerations across key technical domains in which quantum-resilient or PQC solutions are applied, including web browsers, public-key infrastructure (PKI), data encryption, cloud services, and authentication, with prompts designed to facilitate meaningful dialogue about PQ readiness. These capabilities are broadly aligned with the technical domains outlined in the PQCC Capability Heatmap Initial Definition.

This Guide does not include cost as an analysis factor, as organizations vary significantly in how they prioritize cost in decision-making processes.

1.2 How to Use This Guide

The process described in this Guide begins once your organization identifies the need for a PQC solution (product or service). Your organization can evaluate the PQC solution by using the considerations provided in the Analysis Focus Areas and Appendix A. These focus areas can be tailored to your organization and the PQC solution's technical domain. Additionally, tailor the Scoring Procedure to address your organizational priorities or applicable industry and government requirements. Using the tailored focus areas and scoring procedure, your organization can score and analyze PQC solutions. The scoring approach may evolve over time as more analyses are conducted.

Scoring provides a basis to assess the readiness of a PQC solution or compare solutions to inform inventory development, risk management, and procurement decisions within the broader PQC migration effort.

Users of this Guide are encouraged to include as many perspectives from across their organization as possible during analysis. This helps capture a complete picture of the impact of a PQC solution on business and operational activities.

In addition to this analysis, your organization should integrate its existing practices for evaluating cost to make a final decision.

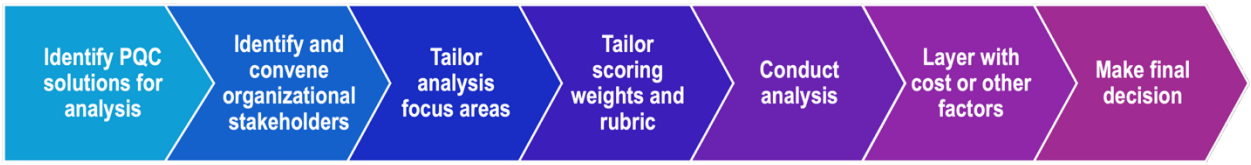

Figure 1: Analysis Workflow

2 Analysis Focus Areas

The following sections describe focus areas that shape scoring of PQC solutions. Focus areas look at technical aspects of PQC capability itself, as well as organizational areas that support and sustain that technology. Some areas may align more closely with your organization's existing evaluation processes. Your organization is encouraged to tailor or add to the focus areas and associated scoring rubric to meet its specific needs.

Appendix A includes question lists to serve as a starting point for analyzing solutions within their technical domain. Your organization can adapt or expand these question lists as they are relevant to each of the focus areas and to your organization's requirements for the PQC solution being analyzed.

2.1 Technical Readiness

Technical readiness assesses the solution's current ability to support PQC in practice. It can be assessed using a combination of the Technology Readiness Level (TRL) framework[2] and the PKI Consortium's Post-Quantum Cryptography Maturity Model (PQCMM)[3], providing a structured way to assess how mature and deployable a solution is. A technical readiness assessment should also consider alignment with modern security architectures, such as Zero Trust, where cryptographic protections are continuously enforced across identities, devices, and network boundaries.

Key considerations:

- Existence of proofs of concept, pilots, or production deployments
- Interoperability and performance validation
- Overall maturity of PQC-enabled products and features
- Alignment with other modern security priorities and capabilities (for example, Zero Trust)

2.2 Crypto Agility

Crypto agility assesses whether the solution can adapt to evolving cryptographic standards. As computing advances, organizations can anticipate changes to cryptographic standards. Moving to a crypto-agile solution is critical for organizations to avoid costly cryptographic migrations in the future. NIST's Cybersecurity White Paper

[2] https://www.nasa.gov/directorates/somd/space-communications-navigation-program/technology-readiness-levels/

[3] https://pkic.org/2025/10/27/defining-quantum-readiness-introducing-the-post-quantum-cryptography-maturity-model/

(CSWP) 39, “Considerations for Achieving Crypto Agility,”[4] and the Crypto Agility Maturity Model (CAMM)[5] are helpful for evaluating this focus area.

Key considerations:

- Presence of crypto-agile architecture
- Ability to update algorithms without rip-and-replace
- Support for hybrid (classical + PQC) mechanisms
- Defined and demonstrated processes for algorithm and key rotation
- Existence of a documented crypto-agility strategy or roadmap

2.3 PQC Standards Alignment

PQC Standards Alignment assesses whether the solution aligns with applicable PQC standards and industry guidance for its technical domain.

Key considerations:

- Alignment with NIST, IETF, and relevant industry standards
- Support for standardized PQC algorithms and protocols
- Coverage across relevant protocols and product lines
- Awareness of and responsiveness to evolving standards and guidance

2.4 Timeline

Timeline assesses the time it will take to realize the PQC modernization benefit associated with the solution. Timeline may depend on both technical elements of the solution’s readiness and the realities of organizational implementation. This focus area is most relevant for solutions addressing quantum threats to confidentiality (for example, harvest now, decrypt later). Timeline should be tailored to the solution being considered as well as organizational priorities.

Key considerations:

- Time until the solution is technically ready for deployment
- Time required for full integration within the organization
- Alignment with the organization’s risk horizon and implementation timelines

[4] https://doi.org/10.6028/NIST.CSWP.39

[5] https://camm.h-da.io/model/

2.5 Integration Fit

Integration fit assesses how easily a solution can be adopted, integrated, and sustained within an organization's environment.

Key considerations:

- Ease (or complexity) of implementation and integration into existing workflows
- Management of the solution through a new or existing vendor
- Usability for operators and end users (low friction, minimal workarounds)
- Impact on existing systems and dependencies
- Alignment with immediate organizational business and operational needs (for example, sensitivity or recency of data handled by the solution)
- Dependence on upstream components or ecosystems that may impact longevity
- Long-term sustainability of the solution within operational environments (for example, 10-30 years)

2.6 Provider Ability to Execute

Provider ability to execute assesses whether the organization providing the solution has the structure, resources, and processes needed to effectively execute and sustain PQC migration now and in the future. Your organization should consider conducting analysis of this focus area for any parties that provide, integrate, or maintain the solution. This may include one or more external vendors or internal teams.

Key considerations:

- Defined PQC strategy, roadmap, and milestones
- Allocation of funding, staffing, and resources
- Ongoing risk monitoring and response processes
- Solution provider's track record and capability to maintain, support, and evolve solutions
- Defined path toward hardened implementations and rollout
- Ability to communicate PQC status, updates, and risks to customers
- Participation in ecosystem collaboration (suppliers, standards bodies, industry groups)

3 Scoring Model

This scoring model provides a structured way to inform PQC migration decisions and compare quantum-resilient solutions.

The scoring procedure involves three main steps. First, identify relative weights for each of the focus areas corresponding to the organization's priorities. Table 1 provides an example set of scoring categories and example percentage weights. These weights are illustrative and should be adjusted based on organizational priorities.

Table 1: Scoring Focus Areas and Example Weights

Focus Area	Example Weight (%)
Technical Readiness The solution exhibits real technical progress and fitness for contractual or operational requirements	25
Crypto Agility The solution exhibits demonstrated ability to adapt to future cryptographic changes	20
PQC Standards Alignment The solution is being developed in line with emerging PQC standards	15
Timeline The solution can be implemented within a desired timeline	15
Integration Fit The solution is easy to implement within existing workflows and is usable at the operational level	15
Provider Ability to Execute The organization providing the solution has the structure, resources, and processes needed to effectively execute and sustain the solution	10
Total	**100**

Second, tailor the scoring rubric to reflect the organization's analysis focus areas. Table 2 shows a notional scoring rubric, using a scale from 1-5 for the Analysis Focus Areas described above. Organizations can tailor the scoring range and qualitative descriptions. Having well-defined and agreed-upon qualitative descriptions is critical to producing a calibrated and meaningful score.

Table 2: Notional Scoring Rubric

Criteria	1	2	3	4	5
Technical Readiness	Initial or basic PQC implementations are available. (TRL 1-3)		PQC capability has been validated in a component or system in a relevant environment. (TRL 4-6)		PQC capability has been proven through testing in an operational environment or in actual operations. (TRL 7-9)
Crypto Agility	Lack of evaluation or exclusion of crypto-agility through design. (CAMM 0)		Crypto-agility is possible within systems, though conditions may not have been met yet to enable it, or systems are prepared for crypto-agility but have not yet fully realized it in active use/changes to cryptography still require some effort. (CAMM 1-2)		Crypto-agility is practiced and demonstrably, effectively, and securely feasible. Solution may show additional advanced capabilities in crypto-agility applied through broader infrastructure. (CAMM 3-4)
PQC Standards Alignment	Little or no adoption of PQC standards.		Some evidence of alignment with PQC standards relevant to the technical domain.		Extensive evidence of alignment with PQC standards relevant to the technical domain.
Timeline	Little or no implementation of solution likely within desired timeline.		Moderate implementation, or implementation will be underway but not in production within desired timeline.		Implementation of solution is achievable within desired timeline.
Integration Fit	Solution is difficult or impossible to integrate or sustain. May conflict with operational realities, dependencies, or require workarounds that do not align with business needs.		Solution is moderately easy to integrate and sustain. May require some workarounds, have many dependencies, or have an unclear/moderate impact on business operations.		Solution is extremely easy to integrate and sustain. Is usable with minimal workarounds, well-designed, and a good fit for business and operational needs.
Provider Ability to Execute	Little or no evidence of provider track record for delivery or quality. May lack PQC governance, and/or have poor customer engagement and PQC ecosystem engagement.		Moderate evidence of provider ability to execute. May have PQC governance and integration plan initiated, with a timeline but lacking specific milestones. Customer engagement is moderate. Minimal engagement with other providers and upstream suppliers on PQ readiness. Provider may not have a proven track record for maintaining and evolving solutions.		Comprehensive evidence of provider ability to execute. Has strong PQC governance and an integration plan, established customer communications, and validated test plans for solution sustainability. Regular collaboration with customers and ecosystem, providing updates on PQC mitigation, planning, and progress.

Third, with the weights and rubric defined, conduct scoring for each of the focus areas. The final quantitative score, adjusted to an organization's weighting system, can be layered with cost analysis and used to compare multiple solutions and inform procurement and migration prioritization decisions.

3.1 Evaluating Analysis Scores

Once you have completed the analysis, you can use the resulting score to support decision-making regarding a single solution or compare multiple solutions from different providers.

This section provides guidance on how to interpret responses from provider(s) about their quantum-resilient solution to determine the appropriate follow-up actions. Not every provider will be far along in their PQC journey, but responses should demonstrate awareness, transparency, and increasing technical maturity over time.

3.1.1 Single Solution Next Steps

Quantitative scoring of quantum-resilient solutions can assist organizations in determining what actions to take in implementing that solution or when conducting follow-on discussions with the solution provider. The following considerations are intended to provide general guidance and should be adapted based on organizational priorities, risk tolerance, and operational context informed by the analysis process. Organizations may choose what constitutes a "high" score in line with these factors as well as the broader ecosystem of available solutions.

3.1.1.1 Considerations for High Scoring Solutions

- Implement or prioritize solutions for pilots or early integration efforts
- Explore opportunities to collaborate with the solution provider to align PQC roadmaps, risks, and timelines
- Incorporate PQC-related expectations into future planning or procurement discussions with the solution provider
- Evaluate the solution provider's role in phased deployment or long-term migration strategies

3.1.1.2 Considerations for Other Solutions

- Determine need for a future review of the solution to track technical or organizational progress
- Encourage the solution provider to conduct further testing or standards alignment
- Identify potential risk exposure associated with the solution and incorporate the solution's progress into ongoing risk monitoring efforts

- Request additional clarity on or encourage the solution provider's PQC planning (may include roadmaps, milestones, and scope)
- Consider mitigation strategies or alternative approaches in place of the solution as appropriate

3.1.2 Multiple Solution Comparison

Scores may also be used to compare solutions from multiple providers. Figure 2 shows an example of what this comparison might look like (not considering cost), including a notional status quo and four solutions for comparison. This score should be used as a decision-support tool, not a strict compliance metric, and should be interpreted alongside qualitative insights from engagement with the solution provider.

Figure 2: Notional Scoring Results for Multiple Solutions and Status Quo

CRITERIA	STATUS QUO	SOLUTION 1	SOLUTION 2	SOLUTION 3	SOLUTION 4	WEIGHT (%)
Technical Readiness	2	3	4	3	5	25
Crypto-Agility	2	4	4	4	5	20
PQC Standards Alignment	1	3	5	3	4	15
Timeline	2	3	3	4	3	15
Integration Fit	2	2	4	4	5	15
Provider Ability to Execute	2	3	3	4	4	10
Weighted Score	1.85	3.05	3.90	3.60	4.45	

Visualizing the scoring comparison can help identify clusters of scores, provide context for the sensitivity of scoring (for example, whether a difference of 0.5 or 1 is significant in selecting a solution), and feed back into the process of weighting focus areas. Your organization may also interpret the results of the score comparison alongside additional considerations, such as cost, before taking next steps.

4 Conclusion

Once your organization has tailored the scoring activities described in this Guide for PQC products and services, it can continue to reuse and refine it in future analyses, measure solution suitability over time, and adjust PQC migration activities accordingly.

As your organization progresses into planning and execution activities for its PQC migration, continued engagement with the providers of PQC solutions will be essential to confirm solution readiness, alignment with emerging standards (including NIST FIPS 203, 204, and 205), workforce impacts, and acquisition pathways. As solutions evolve over time and become integrated into your organization's operations, these engagements should mature from exploratory conversations into structured coordination around pilots, solution acquisition, implementation sequencing, and long-term support.

Ultimately, a successful post-quantum transition will require sustained coordination across internal stakeholders and external partners. By creating a tailored quantitative framework for evaluating PQC solutions, organizations can reduce uncertainty, avoid fragmented migration efforts, and build a foundation for a coordinated, standards-aligned, and resilient transition to post-quantum security.

Appendix A: Technical Domains & Tailored Questions

This section outlines specific technical domains in which cryptographic protocols are most affected by quantum threats. Each domain includes tailored questions to help assess solution readiness, planned migrations, and threat monitoring practices related to post-quantum cryptography.

Web Browsers / Servers

Web browsers and web servers rely on TLS to establish confidentiality and integrity for web communications. Classical public-key algorithms such as RSA and ECC are widely deployed and are vulnerable to cryptographically relevant quantum computers. Support for post-quantum and hybrid TLS is emerging across major platforms, making web traffic one of the earliest and most visible PQC transition areas. Solution providers should be planning for PQC-enabled TLS and crypto-agile update paths.

- What cryptographic algorithms are currently used for securing browser communications (such as TLS and HTTPS)?
- Have you assessed the vulnerability of these algorithms to quantum computing attacks?
- What is your roadmap for supporting post-quantum cryptographic algorithms in your browser and/or server communications?
- How do you monitor for new threats or vulnerabilities related to quantum computing?
- What is your process for updating cryptographic libraries in response to new threats?

VPN / Network Encryption

VPN and network encryption solutions protect organizational traffic traversing untrusted networks such as the internet. These systems rely heavily on public-key cryptography for key establishment and authentication, making them directly exposed to quantum risk. Several solution providers have announced initial support for post-quantum or hybrid key exchange, but deployment coverage varies significantly by product, protocol, and platform. Solution providers should be able to articulate both near-term hybrid support and longer-term migration strategies.

- What encryption algorithms are used for VPN tunnels and network encryption?
- Have you conducted a risk assessment regarding the impact of quantum computing on these algorithms?
- What is your timeline for supporting post-quantum encryption in your VPN products?

- How do you plan to manage key exchange and authentication in a post-quantum environment?
- What is your process for informing customers of new risks or required configuration changes?
- What is the process for adding new quantum-resistant algorithms, as they become available, on the same platform (i.e. without a rip-and-replace)?
- Is there a threat-agility plan in which ciphers and keys are rotated based on detected threats?

Platform Assurance

Platform assurance covers protections for foundational system components such as firmware, boot loaders, hypervisors, and hardware roots of trust (for example, TPMs and secure enclaves). These mechanisms establish that a system starts and runs in a trusted state and that only authorized code is allowed to run. Because platform controls underpin all higher-level security and are often tightly coupled to hardware, they are typically difficult and costly to update once deployed. PQC standards and implementations in this area are still maturing, though post-quantum signatures are becoming viable for firmware signing and secure boot chains.[6] As a result, platform assurance is usually addressed later in the PQC migration lifecycle, particularly during the Execution and Monitoring and Evaluation phases, once inventories are complete and concrete implementation paths are defined.

- What types of hardware-based trust components are included?
- How does the solution integrate hardware and software?
- Where does PQC enforcement and termination occur relative to the customer trust boundary?
- What is your process for updating cryptographic mechanisms in deployed hardware platforms?
- Where are trust anchors stored (TPM, HSM, firmware, secure enclave), and what are the PQC constraints of those components?
- If the platform consists of highly constrained devices (IoT), what explicit measures exist to assure primary trust anchors (for example, secure boot, firmware updates, and code signing)?
- Have you assessed which current hardware modules cannot support PQC algorithms due to performance or architectural constraints?
- How are cryptographic changes tested and validated before deployment?

[6] This work-in-progress internet draft on Adapting Constrained Devices for Post-Quantum Cryptography is one example of the developing standards in this area: https://datatracker.ietf.org/doc/draft-ietf-pquip-pqc-hsm-constrained/. Discussions related to the document are archived at https://mailarchive.ietf.org/arch/browse/pqc/.

- Does the solution consider protections against side-channel and fault attacks?

Code Signing / Patch Management

Code signing and patch management systems ensure the authenticity and integrity of software updates, operating systems, and applications. These mechanisms commonly rely on long-lived signing keys and trust chains, creating elevated risk in a post-quantum context. While PQC code-signing ecosystems are still emerging, solution providers should be evaluating migration paths, coexistence strategies, and the operational impact of replacing signing infrastructures.

- What cryptographic algorithms are used for code signing and patch validation?
- Have you identified vulnerabilities of these algorithms to quantum attacks?
- What is your strategy for transitioning to post-quantum code signing mechanisms?
- How will you ensure backward compatibility and integrity during the transition?
- How do you communicate risks and mitigation strategies to customers regarding code signing?

PKI / CA Management

Public Key Infrastructure allows for authentication, secure communications, device identity, and trust management across most enterprise environments. Many platform solution providers now support PQC algorithms, but large-scale PKI transitions remain complex due to certificate lifecycles, interoperability, and dependency chains. Solution providers should be planning for hybrid certificates and phased migrations aligned with emerging standards.

- What algorithms are currently used for certificate issuance, validation, and revocation?
- How are certificate lifetimes, renewal cycles, and trust anchors being evaluated in light of quantum risk?
- What is your plan for migrating to quantum resilient certificate authorities and certificates?
- How will you manage the coexistence of classical and post-quantum certificates?
- What is your approach to monitoring and responding to new threats in PKI management?
- Are any serial or management interfaces accessible remotely without cryptographic protection, and what is the plan to secure these interfaces as part of platform assurance improvements?

Cloud Service Connectivity

Cloud service connectivity relies on secure channels and identity mechanisms between customers, cloud services, and cloud management planes. These connections typically depend on TLS, PKI, and federated authentication systems, inheriting the same quantum vulnerabilities as web services. While early PQC support may be available in select environments, organizations depend on cloud providers to deliver transparent, standards-aligned migration paths that minimize customer disruption.

- What protocols and cryptographic algorithms are used for connecting to cloud services?
- Have you evaluated the susceptibility of these protocols to quantum attacks?
- What is your plan for supporting post-quantum authentication mechanisms?
- How will you ensure secure migration for cloud services?
- How do you monitor and communicate new cloud service risks in a post-quantum context?

Volume Encryption

Volume encryption protects data at rest on physical and virtual storage systems. While symmetric encryption itself is less affected by quantum computing, the key establishment, key wrapping, and access-control mechanisms used to protect storage systems often rely on public-key cryptography and long-lived trust models. Solution providers should be assessing cryptographic agility, key management dependencies, and risks to long-lived encrypted data.

- What encryption algorithms are used for data at rest?
- Have you assessed the risk of quantum attacks on stored encrypted data?
- What is your roadmap for implementing post-quantum encryption for data at rest?
- How do you plan to handle key management and migration to new algorithms?
- What is your process for updating customers on risks and recommended actions?
- What is the process for adding new quantum-resistant algorithms, as they become available, on the same platform, i.e., without a rip-and-replace?
- Is there a threat-agility plan in which ciphers and keys are rotated based on detected threats?

Internal / User Authentication to Remote Resources

Authentication systems establish user, device, and service identity across enterprise environments. These systems often integrate PKI, federated identity, smart cards, hardware tokens, and VPN authentication. Because authentication failures undermine every dependent system, solution providers should be evaluating PQC impacts across

identity protocols, credential formats, hardware authenticators, and backend trust systems.

- What authentication protocols and cryptographic algorithms are used for remote access?
- Have you evaluated the susceptibility of these protocols to quantum attacks?
- What is your plan for supporting post-quantum authentication mechanisms?
- How will you ensure secure migration for user credentials and authentication systems?
- How do you monitor and communicate new risks related to authentication in a post-quantum context?