QUBIXOR

Qubixor Post-Quantum Maturity Model (QPQMM)

Methodological Framework — Version 1.0

February 2026

Qubixor

qubixor.com

Table of Contents

- Qubixor Post-Quantum Maturity Model (PQMM)
  - Methodological Framework – Version 1.0
- Abstract
- Executive Summary
  - 1. Purpose of the PQMM
  - 2. Why Post-Quantum Readiness Requires a Structured Framework
  - 3. What the PQMM Measures
  - 4. What the PQMM Does Not Measure
  - 5. Intended Audience
  - 6. Key Structural Components of the Model
- 1. Introduction
  - 1.1 Context: Post-Quantum Cryptographic Transition
  - 1.2 Strategic Risk Landscape
  - 1.3 Need for a Structured Maturity Model
  - 1.4 Document Scope and Boundaries
- 2. Conceptual Foundations
  - 2.1 Definition of Post-Quantum Readiness
  - 2.2 Governance vs Technical Exposure
  - 2.3 Crypto-Agility as a Foundational Principle
  - 2.4 Risk Horizon Assumptions
  - 2.5 Model Design Principles
- 3. Normative and Standards Alignment
  - 3.1 Alignment with NIST Post-Quantum Standardization
  - 3.2 Alignment with Cryptographic Governance Standards
  - 3.3 Relationship with ISO 27001 / 27002 Cryptographic Controls
  - 3.4 Complementarity with Existing Cybersecurity Frameworks
  - 3.5 Normative Mapping Table
- 4. Model Architecture
  - 4.1 Structural Overview
  - 4.2 Dimensions of the PQMM

5. Maturity Levels Framework
- 5.1 Level Structure Overview
- 5.2 Level 0 – Unaware / Non-Structured
- 5.3 Level 1 – Initial Awareness
- 5.4 Level 2 – Structured Assessment
- 5.5 Level 3 – Managed Transition
- 5.6 Level 4 – Strategically Integrated

6. Scoring Methodology
- 6.1 Scoring Scale Definition
- 6.2 Dimension-Level Scoring Logic
- 6.3 Weighting Model
- 6.4 Aggregation Formula
- 6.5 Consistency Controls
- 6.6 Sensitivity Considerations

7. Interpretation Framework
- 7.1 Interpreting the Global Score
- 7.2 Interpreting Dimension Imbalances
- 7.3 Risk Exposure vs Organizational Maturity
- 7.4 Board-Level Interpretation Guidance
- 7.5 Technical vs Strategic Interpretation
- 7.6 Narrative Interpretation Examples

8. Migration Path Framework
- 8.1 Phased Transition Model

9. Sectoral Application Framework
- 9.1 Financial Sector
- 9.2 Critical Infrastructure
- 9.3 Public Sector Organizations
- 9.4 SaaS and Cloud-Native Organizations

10. Data Collection and Aggregation Methodology
- 10.1 Data Types Collected
- 10.2 Anonymization Principles
- 10.3 Aggregation Logic
- 10.4 Statistical Limitations

10.5 Benchmark Construction Method
11. Model Assumptions and Limitations
11.1 Core Assumptions
11.2 Temporal Assumptions
11.3 Organizational Assumptions
11.4 Known Limitations
11.5 Non-Applicability Cases
12. Model Governance
12.1 Versioning Policy
12.2 Revision Triggers
12.3 Update Cycle
12.4 External Review Possibilities
12.5 Transparency Commitments
13. Comparative Positioning
13.1 Differences from Generic Cyber Maturity Models
13.2 Complementarity with Enterprise Risk Frameworks
13.3 Non-Substitution Statement
14. Implementation Guidance
14.1 Organizational Preparation
14.2 Internal Stakeholder Engagement
14.3 Reporting to Executive Leadership
14.4 Integration with Enterprise Risk Management
15. Conclusion
15.1 Strategic Implications
15.2 Long-Term Governance Outlook
15.3 Continuous Adaptation Imperative
16. Practical adoption steps
Annex A – Glossary
Annex B – Formal Definitions of Key Concepts
Annex C – Normative References
Annex D – Example Radar Visualization Template
Annex E – Example Executive Reporting Template

Qubixor Post-Quantum Maturity Model (PQMM)

Methodological Framework – Version 1.0

Document type: Methodological Framework
Version: 1.0
Publication date: February 2026
Publisher: Qubixor

Abstract

This document defines the Qubixor Post-Quantum Maturity Model (PQMM), a structured framework for assessing organizational readiness for the transition to post-quantum cryptography (PQC). The framework is designed to support governance and risk management decisions by providing a reproducible, multi-dimensional maturity assessment aligned with widely recognized standardization and regulatory themes. The PQMM does not constitute a certification scheme, an audit of cryptographic implementations, or a guarantee of compliance with any specific regulation. The document specifies the model's conceptual foundations, its five dimensions (Governance, Cryptography, Infrastructure, Transition, Awareness), a five-level maturity scale, a weighted scoring methodology yielding a Quantum Readiness Index (QRI), and the assumptions and limitations governing the model's use. It is intended for security and risk leaders, compliance functions, and executive leadership who require a formal, citable reference for post-quantum readiness discussions. The framework is sector-agnostic and relies on organizational self-disclosure; applicability to highly classified or restricted environments is not assumed without adaptation.

Executive Summary

1. Purpose of the PQMM

The PQMM provides a structured, repeatable method to evaluate an organization's posture with respect to post-quantum cryptographic transition. Its purpose is to support internal governance, risk prioritization, and communication with stakeholders by mapping organizational practices and controls onto a defined maturity scale and a numerical index (QRI). The framework is not intended to replace cryptographic audits, penetration testing, or formal compliance assessments.

2. Why Post-Quantum Readiness Requires a Structured Framework

The move from current public-key cryptography to algorithms resistant to quantum computing involves technical, organizational, and governance dimensions. Absent a structured model, organizations lack a common language and a consistent basis for measuring progress. A maturity framework allows comparison over time and supports resource allocation and reporting without implying a single “correct” migration path.

3. What the PQMM Measures

The PQMM measures the presence and maturity of governance, process, and planning elements that support post-quantum readiness. It evaluates: (1) governance and policy; (2) cryptographic inventory and resilience; (3) infrastructure and vendor readiness; (4) transition planning and dependencies; (5) awareness and training. Each dimension is assessed via a defined set of controls; control-level results are aggregated by dimension and then combined into a single Quantum Readiness Index (QRI) on a 0–100 scale, mapped to five maturity levels.

4. What the PQMM Does Not Measure

The PQMM does not measure the cryptographic strength of deployed systems, the correctness of implementations, or the effectiveness of technical controls. It does not attest to compliance with any specific regulation or standard. It does not evaluate quantum computing capability or the timeline of quantum threats. Conclusions about residual risk or fitness for a particular use case require additional analysis beyond the model.

5. Intended Audience

The document is intended for: security and risk leaders responsible for PQC strategy; compliance and audit functions preparing for regulatory expectations; IT and infrastructure teams involved in cryptographic inventory and migration planning; and executive leadership requiring a formal, neutral reference for board or regulatory communication.

6. Key Structural Components of the Model

The model comprises: (1) five dimensions with explicit scope and evaluation units; (2) a control set (essential and full) used to score each dimension; (3) a 0–100 Quantum Readiness Index (QRI) with a defined aggregation formula and dimension weights; (4) five maturity levels (0–4) with observable characteristics; (5) two assessment modes (Quick

and Complete) differing in control coverage and scoring granularity. Versioning, assumptions, and limitations are documented within the framework.

1. Introduction

1.1 Context: Post-Quantum Cryptographic Transition

Current widely deployed public-key cryptography (e.g., RSA, ECDH, ECDSA) is vulnerable to attacks using sufficiently capable quantum computers. Standardization bodies have published or are publishing post-quantum cryptographic standards (e.g., NIST FIPS 203, 204, 205). Organizations that rely on long-term confidentiality or integrity of data may need to plan for adoption of these algorithms. The transition touches policy, inventory, infrastructure, planning, and awareness; it is not solely a technical upgrade.

1.2 Strategic Risk Landscape

Risks include: exposure of currently encrypted data if it is harvested and decrypted later (Harvest Now, Decrypt Later); inability to meet future regulatory or contractual requirements; and operational disruption if migration is delayed until mandatory. The PQMM does not quantify these risks; it assesses the organizational structures and processes that support informed decision-making and migration readiness.

1.3 Need for a Structured Maturity Model

Maturity models are used in cybersecurity and risk management to compare organizations, track progress, and align stakeholders. A structured model for post-quantum readiness provides a common reference, reduces ambiguity in reporting, and supports prioritization. The PQMM is designed to be reproducible (same inputs yield same outputs) and to separate governance maturity from technical cryptographic exposure where possible.

1.4 Document Scope and Boundaries

This document defines the PQMM methodology: dimensions, controls, scoring, maturity levels, interpretation, and limitations. It does not prescribe migration timelines, product choices, or compliance strategies. The scope is organizational readiness as evidenced by policies, inventories, roadmaps, and awareness; it excludes direct verification of cryptographic implementations. Geographic and sector-specific regulations are referenced only in general terms unless a specific citation is given.

2. Conceptual Foundations

2.1 Definition of Post-Quantum Readiness

Post-quantum readiness (in this framework) denotes the extent to which an organization has put in place governance, inventory, infrastructure, transition planning, and awareness necessary to make informed decisions about adopting post-quantum cryptographic standards and to execute a controlled migration when chosen. Readiness is therefore a function of organizational maturity, not of the current cryptographic strength of any single system.

2.2 Governance vs Technical Exposure

The PQMM distinguishes between:

- **Governance maturity:** Existence and clarity of policies, accountability (e.g., RACI), risk registers, budgets, and regulatory watch. This is assessed primarily in the Governance dimension and reflected in other dimensions where ownership and process are evaluated.
- **Technical exposure:** The actual use of vulnerable algorithms, key lengths, or protocols. The PQMM does not measure technical exposure directly; it assesses whether the organization has inventory, classification, and roadmaps that would support exposure analysis.

A high governance score does not imply low technical exposure; a low governance score does not imply high exposure. The two are complementary views.

2.3 Crypto-Agility as a Foundational Principle

Crypto-agility (see Annex B) is the ability to replace or add cryptographic primitives without redesigning systems. The PQMM treats crypto-agility as an enabler of controlled PQC migration and assesses it within the Cryptography and Infrastructure dimensions (e.g., centralized cipher management, key management architecture, upgradeability). Maturity Level 3 and above assume measurable progress toward crypto-agile design.

2.4 Risk Horizon Assumptions

The model assumes that organizations are planning over a multi-year horizon and that standardization (e.g., NIST) and regulatory guidance will continue to evolve. It does not assume a specific date by which quantum threats will materialize or by which migration

must be complete. Time-bound assumptions in scoring (e.g., presence of a milestoned roadmap) reflect planning maturity, not a fixed deadline.

2.5 Model Design Principles

1. **Neutrality:** The framework does not favour specific vendors, products, or migration strategies. Controls are expressed in terms of outcomes and artefacts, not technologies.
2. **Reproducibility:** The same set of responses, under the same assessment mode and version, produces the same QRI and maturity level.
3. **Scalability:** The same structure applies to organizations of different sizes and sectors; control applicability may be interpreted in context without changing the scoring logic.
4. **Sector-agnostic design:** No dimension or control is defined exclusively for a single sector. Sectoral guidance is provided separately (Section 9) as application notes, not as part of the core scoring.

3. Normative and Standards Alignment

3.1 Alignment with NIST Post-Quantum Standardization

The PQMM uses NIST post-quantum standardization as the technical reference for what “post-quantum” and “quantum-resistant” mean in practice. Specifically, the framework assumes that adoption or planned adoption of mechanisms such as those specified in FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA), or equivalent standardized algorithms, constitutes the target state. The model does not certify conformity to NIST standards; it assesses whether the organization has governance, inventory, and roadmaps oriented toward such adoption.

3.2 Alignment with Cryptographic Governance Standards

Cryptographic governance is addressed in international standards such as ISO/IEC 27001 and ISO/IEC 27002 (cryptographic controls). The PQMM’s Governance dimension overlaps conceptually with control objectives related to policy, risk assessment, and asset management. The framework does not claim coverage of all ISO 27001/27002 controls; it focuses on those relevant to post-quantum planning and migration.

3.3 Relationship with ISO 27001 / 27002 Cryptographic Controls

ISO/IEC 27002 includes controls for cryptographic key management, use of cryptography, and secure development. The PQMM dimensions (especially Cryptography and Infrastructure) address similar themes in the context of PQC transition. Alignment is at the level of control objectives (e.g., inventory, policy, key management), not one-to-one control mapping. Use of the PQMM does not substitute for an ISO 27001 certification or gap assessment.

3.4 Complementarity with Existing Cybersecurity Frameworks

The PQMM is intended to complement, not replace, existing risk and security frameworks (e.g., NIST Cybersecurity Framework, sector-specific frameworks). Organizations may map PQMM dimensions to their existing control sets for reporting; the framework does not require adoption of a particular overarching framework.

3.5 Normative Mapping Table

The following table indicates the nature of alignment between PQMM dimensions and selected normative themes. “Direct” indicates a clear overlap in scope; “Partial” indicates partial overlap or dependency on interpretation; “Complementary” indicates that the PQMM adds a PQC-specific angle to a broader theme. The table integrates NIST post-quantum standards finalized in 2024 (FIPS 203 ML-KEM, FIPS 204 ML-DSA, FIPS 205 SLH-DSA) and European/national guidance (e.g. ANSSI migration guidance).

PQMM dimension	NIST PQC (FIPS 203/204/205, 2024)	ISO 27001/27002 (crypto)	NIS2 / DORA type themes	ANSSI / national PQC guidance
Governance	Partial (migration planning)	Partial	Direct (governance, risk, reporting)	Partial (strategy, ownership)
Cryptography	Direct (algorithm adoption, inventory)	Direct	Partial	Direct (recommendations, migration)
Infrastructure	Partial (deployment, upgradability)	Partial	Partial	Partial (infrastructure readiness)

PQMM dimension	NIST PQC (FIPS 203/204/205, 2024)	ISO 27001/27002 (crypto)	NIS2 / DORA type themes	ANSSI / national PQC guidance
Transition	Direct (roadmap, hybrid deployment)	Complementary	Partial	Direct (migration phases)
Awareness	Complementary	Complementary	Partial	Complementary

This table is for conceptual reference only. It does not imply formal endorsement by any standards body or regulator. For precise normative references, see Annex C.

Intellectual independence. The PQMM is an independent methodological framework developed by Qubixor. It does not represent the official position of any governmental or regulatory authority. References to NIST, ANSSI, ENISA, NIS2, DORA, or other bodies indicate alignment with themes or standards those entities publish; they do not imply endorsement by them.

4. Model Architecture

4.1 Structural Overview

The PQMM consists of five dimensions. Each dimension is evaluated through a set of controls. Control-level scores are aggregated to produce a dimension score; dimension scores are combined using fixed weights to produce the Quantum Readiness Index (QRI). The QRI is mapped to one of five maturity levels. Two assessment modes are defined: Quick Mode (essential controls only) and Complete Mode (full control set), with consistent aggregation rules.

Scoring flow (for methodological visuals): A simple diagram can represent the flow as: *Controls (per dimension) → dimension score (0–100) → weighted sum → QRI (0–100) → maturity level (0–4).* The five dimensions form the inputs to the aggregation; the radar chart (Annex D) is the usual visual for dimension-level scores alongside the single QRI.

4.2 Dimensions of the PQMM

4.2.1 Governance

4.2.1.1 Formal Definition

The Governance dimension evaluates the extent to which the organization has defined accountability, policy, risk management, and resource allocation for post-quantum cryptographic transition. It addresses the presence and clarity of structures and processes that enable informed decision-making and oversight.

4.2.1.2 Scope

Organizational structures, accountability mechanisms (e.g., RACI), strategic oversight, risk registers, budget and sponsorship, and regulatory/standards monitoring related to PQC.

4.2.1.3 Explicit Inclusions

Formal cryptographic or information security policy; post-quantum or HNDL risk register with identified owners; RACI or equivalent for cryptography, PKI, and key management; data classification including confidentiality horizon; dedicated or allocated budget for PQC initiatives; regulatory and standards watch (e.g., NIST, ENISA, sectoral mapping).

4.2.1.4 Explicit Exclusions

Operational implementation details of cryptography; technical design of key management systems; vendor selection or product evaluation.

4.2.1.5 Evaluation Unit

The dimension is evaluated at the level of the organization (or defined scope). The unit of evaluation is the presence and maturity of governance artefacts and assigned responsibilities, not the technical correctness of cryptographic implementations.

4.2.2 Cryptography

4.2.2.1 Formal Definition

The Cryptography dimension evaluates the organization’s cryptographic asset inventory, classification of data by confidentiality horizon, TLS and key management policies, and progress toward post-quantum or hybrid deployment (e.g., pilots, roadmaps).

4.2.2.2 Scope

Cryptographic inventory (CBOM-style); data classification by sensitivity and horizon; TLS policy and cipher management; key management architecture (KMS/HSM); post-quantum or hybrid roadmap and pilots; archival and long-term protection strategy.

4.2.2.3 Explicit Inclusions

Centralized or consolidated cryptographic inventory with defined coverage; classification of data by confidentiality horizon; formalized TLS policy and enforcement; roadmap for hybrid TLS/KEM or PQC adoption with milestones; centralized key management; PQC pilots using standardized algorithms; strategy for long-term cryptographic protection of archived data.

4.2.2.4 Explicit Exclusions

Vendor-specific product choices; cryptographic algorithm design; formal verification of implementations.

4.2.2.5 Evaluation Unit

The dimension is evaluated at the level of the organization's cryptographic governance and planning. The unit is the existence and maturity of inventory, policy, and roadmap artefacts, not the cryptographic strength of each asset.

4.2.3 Infrastructure

4.2.3.1 Formal Definition

The Infrastructure dimension evaluates the extent to which systems and vendor relationships support cryptographic upgradability, consistent TLS and certificate management, and alignment with PQC roadmaps (e.g., cloud KMS/HSM, OTA updatability).

4.2.3.2 Scope

TLS termination and cipher management; certificate and key inventory across infrastructure; cloud and on-premise key management with PQC roadmap; over-the-air or equivalent cryptographic upgradability; VPN and network crypto profiles; certificate lifecycle and exhaustion monitoring.

4.2.3.3 Explicit Inclusions

Consistent TLS termination architecture; centralized cipher management (e.g., via IaC); certificate inventory across in-scope systems; cloud KMS/HSM with documented PQC roadmap; OTA or equivalent crypto-upgradability where applicable; VPN and related profiles aligned with hybrid/PQC; monitoring of certificate expiration and exhaustion.

4.2.3.4 Explicit Exclusions

Detailed network topology; performance or capacity planning; vendor-specific implementation details beyond roadmap and capability.

4.2.3.5 Evaluation Unit

The dimension is evaluated at the level of the organization's infrastructure governance and documented capabilities. The unit is the presence and maturity of architectural and operational artefacts that enable PQC migration.

4.2.4 Transition

4.2.4.1 Formal Definition

The Transition dimension evaluates the presence and quality of migration roadmaps, prioritization (e.g., by HNDL risk), hybrid deployment strategy, and performance or integration testing related to PQC.

4.2.4.2 Scope

Milestoned PQC migration roadmap; prioritization criteria (e.g., HNDL exposure, criticality); hybrid deployment approach by domain or system type; performance and compatibility testing; phased rollout strategy.

4.2.4.3 Explicit Inclusions

Documented PQC roadmap with milestones; prioritization of migration by risk or business impact; hybrid deployment strategy per domain; testing of KEM/signature performance or compatibility; phased hybrid deployment plan.

4.2.4.4 Explicit Exclusions

Exact project timelines (unless used only as evidence of planning maturity); vendor roadmaps; detailed technical migration steps.

4.2.4.5 Evaluation Unit

The dimension is evaluated at the level of the organization's transition planning. The unit is the existence and clarity of roadmap, prioritization, and deployment artefacts.

4.2.5 Awareness

4.2.5.1 Formal Definition

The Awareness dimension evaluates the extent to which the organization has put in place executive briefing, technical training, and external engagement related to post-quantum cryptography and quantum risk.

4.2.5.2 Scope

Executive-level awareness of quantum and PQC risk; technical training on PQC for relevant roles; participation in industry or standards initiatives.

4.2.5.3 Explicit Inclusions

Executive briefings on quantum risk and PQC; technical PQC training programs or materials; external engagement (e.g., fora, standards participation, information sharing).

4.2.5.4 Explicit Exclusions

Depth or quality of technical knowledge; certification of individuals; marketing or external communication content.

4.2.5.5 Evaluation Unit

The dimension is evaluated at the level of the organization. The unit is the presence of briefing, training, and engagement activities, not the measured competence of individuals.

5. Maturity Levels Framework

5.1 Level Structure Overview

The PQMM defines five maturity levels, numbered 0 to 4. Each level corresponds to a QRI score band. The level is determined solely by the QRI value; there is no separate qualitative override. The bands are: Level 0 (QRI 0–20); Level 1 (20–40); Level 2 (40–60); Level 3 (60–80); Level 4 (80–100).

5.2 Level 0 – Unaware / Non-Structured

Organizational characteristics: No formal recognition of post-quantum risk at leadership level; no dedicated accountability for cryptography or PQC; no timeline or roadmap consideration.

Governance posture: No cryptographic policy that references PQC or quantum risk; no risk register entries for HNDL or PQC; no assigned owner for cryptographic or key management decisions.

Cryptographic inventory maturity: No centralized cryptographic inventory; no systematic data classification by confidentiality horizon.

Residual risk profile: Organization has not assessed exposure; no basis for prioritization. Residual exposure is undefined from the model's perspective.

Observable indicators: Absence of policy, risk register, RACI, and inventory artefacts; no evidence of executive briefing or PQC budget.

5.3 Level 1 – Initial Awareness

Organizational characteristics: General awareness of post-quantum risk; monitoring of NIST or ecosystem developments; no structured organizational assessment or formal roadmap.

Governance posture: Some awareness at leadership level; possible ad-hoc risk discussion; no formal policy or RACI; no dedicated budget.

Cryptographic inventory maturity: No comprehensive inventory; possibly partial or informal lists; no formal data classification by horizon.

Residual risk profile: Risk is recognized but not systematically mapped; prioritization is not possible on a structured basis.

Observable indicators: Evidence of monitoring (e.g., attendance at events, reading); no formal policy, no milestoned roadmap, no CBOM.

5.4 Level 2 – Structured Assessment

Organizational characteristics: Cryptographic inventory (CBOM) initiated; risk mapping performed; executive visibility on PQC; defined ownership for at least some cryptographic domains.

Governance posture: Documented policy or risk register referencing PQC; RACI or equivalent for crypto/PKI/KMS; data classification including horizon; some budget or sponsorship.

Cryptographic inventory maturity: Inventory covering a defined scope; TLS policy documented; roadmap may exist but not yet detailed or milestoned.

Residual risk profile: Organization can identify critical assets and high-exposure areas; prioritization is possible; migration not yet systematically planned.

Observable indicators: Existence of CBOM, risk register entries, RACI, data classification; executive briefing or board-level visibility; no full crypto-agility or controlled migration yet.

5.5 Level 3 – Managed Transition

Organizational characteristics: Migration strategy drafted; governance defined and sustained; crypto-agility in place or in progress (ability to change primitives without full

redesign).

Governance posture: Sustained policy, risk register, and RACI; regulatory and standards watch; quantified PQC risk where applicable; clear budget and sponsorship.

Cryptographic inventory maturity: Inventory with high coverage; TLS and KMS policies enforced; hybrid or PQC pilots in progress; roadmap with milestones.

Residual risk profile: Prioritized migration path; residual exposure is understood and managed within the roadmap; crypto-agility reduces lock-in.

Observable indicators: Milestoned roadmap; hybrid deployment strategy; centralized cipher/key management; PQC pilots; crypto-agility design in critical systems.

5.6 Level 4 – Strategically Integrated

Organizational characteristics: Roadmap aligned with standardization timelines; crypto-agile architecture where critical; vendor and ecosystem reviewed; capabilities embedded in governance and planning cycles.

Governance posture: PQC integrated into risk and strategy; regular review of roadmap and risk; full accountability and budget; external engagement and standards alignment.

Cryptographic inventory maturity: Comprehensive inventory; hybrid or PQC adoption in critical paths; archival strategy defined; continuous monitoring of certificate and key lifecycle.

Residual risk profile: Migration under way or planned with clear ownership; residual exposure consciously accepted or mitigated; organization is prepared to adapt as standards evolve.

Observable indicators: Documented alignment with NIST or equivalent timelines; crypto-agility demonstrated; vendor PQC readiness assessed; continuous monitoring and update processes.

6. Scoring Methodology

6.1 Scoring Scale Definition

Control-level scoring is binary (implemented / not implemented) for Quick Mode. In Complete Mode, a portion of the score may reflect quality of free-text responses (relevance, clarity, specificity) in addition to binary implementation status. Dimension-

level scores are normalized to a common scale (e.g., 0–100 per dimension). The global QRI is the weighted sum of dimension scores, normalized to 0–100.

Score values: Each control contributes to its dimension score. The aggregation uses tag weights (e.g., Direct 1.00, Migration 0.95, Hygiene 0.85) and criticality weights (e.g., Critical 1.15, High 1.00, Medium 0.90, Low 0.80) so that controls are weighted by relevance and criticality. Exact weights are defined in the assessment configuration and are fixed for a given framework version.

6.2 Dimension-Level Scoring Logic

Within each dimension, control scores are combined using a weighted average. Weights reflect the tag (Direct, Migration, Hygiene) and criticality (Critical, High, Medium, Low) assigned to each control. The result is a dimension score in the same scale as the global QRI (0–100). Missing or non-applicable controls are handled by excluding them from the denominator for that dimension so that the dimension score reflects only the applicable set.

6.3 Weighting Model

The five dimensions have the following weights in the global QRI: Governance 18%; Cryptography 24%; Infrastructure 20%; Transition 20%; Awareness 18%. These weights reflect a design assumption that cryptographic inventory and resilience (Cryptography) and infrastructure readiness (Infrastructure, Transition) are central to migration capability, while Governance and Awareness are enablers. The weights are fixed for the framework version and are not tuned per organization or sector.

6.4 Aggregation Formula

Let $(d_1, \ldots, d_5)$ denote the dimension scores (each in 0–100) for Governance, Cryptography, Infrastructure, Transition, and Awareness respectively. Let $(w_1 = 0.18)$, $(w_2 = 0.24)$, $(w_3 = 0.20)$, $(w_4 = 0.20)$, $(w_5 = 0.18)$. Then:

$$ \text{QRI} = \sum_{i=1}^{5} w_i \cdot d_i $$

The QRI is therefore in the range 0–100. Maturity level is derived from QRI bands: 0–20 → Level 0; 20–40 → Level 1; 40–60 → Level 2; 60–80 → Level 3; 80–100 → Level 4.

6.5 Consistency Controls

The same assessment mode (Quick or Complete) and the same framework version must be used when comparing scores over time or across organizations. Control sets differ

between modes; QRI may differ for the same organization between modes. Reproducibility holds only within a single mode and version.

6.6 Sensitivity Considerations

Small changes in a few controls can shift the QRI by a few points; near boundary (e.g., 38–42) a small change can change the maturity level. Users should interpret the level as a band, not a precise classification. Dimension-level scores provide more nuance than the single QRI.

7. Interpretation Framework

7.1 Interpreting the Global Score

A low QRI indicates that the organization has not yet put in place the governance, inventory, and planning artefacts that the model treats as indicators of readiness. It does not directly measure technical exposure or residual risk. A high QRI indicates that the organization has documented policies, inventories, roadmaps, and awareness activities that meet the control criteria; it does not attest to the correctness of implementations or to compliance with any regulation.

7.2 Interpreting Dimension Imbalances

Imbalance across dimensions (e.g., high Cryptography, low Governance) suggests that technical progress may outpace oversight and resource allocation, or conversely that governance exists without corresponding inventory or roadmap. Such imbalance does not imply that one dimension is “more important”; it indicates where additional focus may be needed for a balanced readiness posture.

7.3 Risk Exposure vs Organizational Maturity

The model does not output a risk exposure metric. Maturity (and QRI) reflects process and artefact maturity, not the actual exposure of assets. An organization with high maturity may still have significant exposure if migration is not yet executed; an organization with low maturity may have low exposure by chance or scope. Interpretation for risk decisions should combine the PQMM output with separate exposure or impact analysis.

7.4 Board-Level Interpretation Guidance

For boards and executive leadership, the QRI and level can be presented as: (1) a snapshot of organizational readiness as defined by the framework; (2) a basis for tracking progress over time; (3) a common reference for resource and priority discussions. The framework does not allow the conclusion that the organization is “secure” or “compliant”; it allows the conclusion that defined governance and planning elements are in place to a certain degree.

7.5 Technical vs Strategic Interpretation

Technical audiences may use dimension and control-level detail to identify gaps and plan remediation. Strategic audiences may use the overall level and QRI for reporting and comparison. The model does not support conclusions about the effectiveness of specific controls or the suitability of specific technical choices.

7.6 Narrative Interpretation Examples

The following scenarios illustrate how to read the scores in practice:

- **High QRI but one dimension clearly lower:** For example, Cryptography and Infrastructure are strong (e.g. 75–85) but Awareness is 35. This suggests technical and infrastructure readiness outpace organizational awareness and training. The priority is not more controls in the strong dimensions but closing the awareness gap so that decisions and communication are aligned with the actual posture.
- **Rough balance across dimensions but QRI in the 40–50 band:** The organization has a structured approach in all five dimensions but has not yet reached managed transition (e.g. no milestoned roadmap, no hybrid pilots). Interpretation: baseline is in place; the next step is to move from “we know what we have” to “we have a plan and we are executing it,” especially in Transition and Cryptography.
- **High Governance, lower Cryptography and Infrastructure:** Governance and Awareness scores are high (e.g. 70+), but Cryptography and Infrastructure are in the 30–45 range. This indicates that policy and ownership exist without yet being backed by a mature cryptographic inventory, TLS/KMS alignment, or infrastructure roadmap. The message for leadership: governance is ready; the bottleneck is technical execution and inventory—resource and priority should focus there.

8. Migration Path Framework

8.1 Phased Transition Model

The following phases describe a logical sequence for building readiness. They are not calendar phases; duration depends on organizational context.

Phase 0 – Awareness

Objectives: Establish leadership and stakeholder awareness of post-quantum risk and of the need for a structured response.

Required artefacts: Evidence of briefing or training; assignment of accountability (even if initial).

Governance checkpoints: Recognition of PQC in risk or strategy discussions.

Indicators of completion: Documented awareness activity; named owner or sponsor.

Phase 1 – Cryptographic Inventory

Objectives: Build a cryptographic asset inventory (CBOM) and classify data by confidentiality horizon to enable prioritization.

Required artefacts: Inventory covering a defined scope; data classification policy or matrix including horizon.

Governance checkpoints: Inventory ownership; linkage to risk register.

Indicators of completion: Inventory with defined coverage; classification applied to critical data.

Phase 2 – Crypto-Agility Enablement

Objectives: Establish architecture and processes that allow cryptographic primitives to be updated without full system redesign.

Required artefacts: Centralized cipher and key management; documented upgrade path; TLS and KMS policy.

Governance checkpoints: Architecture review; alignment with roadmap.

Indicators of completion: Centralized management in place; OTA or equivalent upgradability where applicable.

Phase 3 – Controlled Migration

Objectives: Execute a prioritized migration plan using hybrid or PQC mechanisms in line with standardization.

Required artefacts: Milestoned roadmap; hybrid deployment strategy; pilot results; performance and compatibility testing.

Governance checkpoints: Regular roadmap review; risk register updates; budget and resource allocation.

Indicators of completion: Pilots completed; rollout plan for critical systems; monitoring in place.

Phase 4 – Continuous Monitoring

Objectives: Integrate PQC into ongoing governance, lifecycle management, and vendor management.

Required artefacts: Continuous inventory and certificate monitoring; vendor PQC readiness assessment; update to policies and roadmaps as standards evolve.

Governance checkpoints: Integration with risk and compliance cycles; external engagement.

Indicators of completion: Sustained monitoring; regular review of roadmap and risk; adaptation to new standards.

9. Sectoral Application Framework

9.1 Financial Sector

Typical exposure profile: High reliance on cryptography for transactions, identity, and data protection; regulatory expectations (e.g., DORA) on ICT risk and resilience.

Governance complexity: Often high; existing risk and compliance frameworks; need to map PQMM to regulatory control sets.

Migration constraints: Legacy systems; third-party dependencies; certification and audit requirements.

PQMM-specific priorities: Governance and Transition dimensions for roadmap and regulatory alignment; Cryptography and Infrastructure for inventory and key management.

9.2 Critical Infrastructure

Typical exposure profile: Operational technology and long-lifecycle systems; potential HNDL exposure for sensitive operational data.

Governance complexity: Sector-specific regulations (e.g., NIS2); multiple stakeholders; safety and availability constraints.

Migration constraints: Long upgrade cycles; vendor dependency; need for hybrid or gradual migration.

PQMM-specific priorities: Transition and Infrastructure for roadmap and upgradability; Governance for risk register and accountability.

9.3 Public Sector Organizations

Typical exposure profile: Citizen and state data; long-term archival; compliance with national and EU frameworks.

Governance complexity: Procurement and standardization constraints; national cybersecurity guidance (e.g., ANSSI).

Migration constraints: Budget cycles; centralized or shared services; certification requirements.

PQMM-specific priorities: Governance for policy and regulatory watch; Cryptography and Transition for inventory and roadmap alignment with national timelines.

9.4 SaaS and Cloud-Native Organizations

Typical exposure profile: Customer data in cloud; TLS and API security; dependency on cloud provider crypto capabilities.

Governance complexity: Variable; may be more agile; compliance (e.g., SOC 2, sectoral) may apply.

Migration constraints: Provider roadmap dependency; multi-tenant considerations; key management boundaries.

PQMM-specific priorities: Infrastructure and Cryptography for provider and key management; Transition for roadmap alignment with provider and standards.

10. Data Collection and Aggregation Methodology

10.1 Data Types Collected

The PQMM assessment collects: (1) responses to control-level questions (binary and, in Complete Mode, free text); (2) optional organizational context (sector, size band) for

benchmarking; (3) no direct access to systems or cryptographic material. All data is provided by the organization (self-disclosure).

10.2 Anonymization Principles

Where data is used for benchmarking or research: identifiers are removed or pseudonymized; aggregation is at group level (e.g., sector, size); no single organization is identifiable in published benchmarks. Participation in benchmarking may be optional.

10.3 Aggregation Logic

Benchmark aggregates (e.g., median QRI by sector) are computed from assessments that share the same framework version and assessment mode. Aggregation is descriptive (e.g., median, quartiles); no statistical inference of representativeness is made unless explicitly stated and methodologically documented.

10.4 Statistical Limitations

Benchmarks depend on the population of participating organizations. They are not necessarily representative of a sector or geography. Sample size and selection bias are not controlled by the framework. Use of benchmarks for comparison is at the user's discretion.

10.5 Benchmark Construction Method

Where benchmarks are published: the construction method (population, filters, aggregation, version, mode) is documented. Benchmarks are updated periodically; date and method are stated so that users can assess relevance.

11. Model Assumptions and Limitations

11.1 Core Assumptions

The model assumes that: (1) organizations can and will provide accurate self-disclosure; (2) the control set and weights reflect a plausible view of readiness that is consistent across assessments; (3) standardization (e.g., NIST) and regulatory themes will continue to evolve and the framework will be updated accordingly; (4) the primary use is organizational self-assessment and progress tracking, not external certification.

11.2 Temporal Assumptions

The model does not assume a specific date for quantum threats or for migration completion. References to “future” or “long-term” are relative. Control criteria that refer to roadmaps or timelines assess the presence of planning, not the adequacy of dates.

11.3 Organizational Assumptions

The model assumes an organization (or defined scope) with identifiable governance, systems, and processes. It does not assume a particular size, sector, or structure; applicability to very small or highly distributed organizations may require interpretation of “organization” and control scope.

11.4 Known Limitations

- The PQMM does not substitute for a cryptographic audit, penetration test, or compliance assessment.
- Results depend on the accuracy and completeness of organizational disclosure.
- The model does not verify the correctness of cryptographic implementations or the effectiveness of controls.
- The framework does not attest to compliance with any regulation or standard.
- Dimension weights are fixed and may not reflect every organization’s risk profile.
- Benchmark data, when used, may not be representative.

11.5 Non-Applicability Cases

The framework is not designed for: (1) highly classified or national security environments without adaptation; (2) contexts where disclosure of control presence is restricted; (3) use as a sole basis for contractual or regulatory compliance; (4) evaluation of individual products or vendors beyond their role in organizational readiness.

12. Model Governance

12.1 Versioning Policy

The framework is versioned (e.g., 1.0). Major version changes may introduce structural changes (dimensions, controls, aggregation); minor version changes may clarify wording

or add controls without changing aggregation. Deprecated versions are documented; users are encouraged to use the current version for new assessments.

12.2 Revision Triggers

Revisions may be triggered by: (1) significant changes in standardization (e.g., new NIST standards or revisions); (2) user feedback and methodological review; (3) regulatory or market evolution; (4) internal governance decision. Changes are documented in release notes.

12.3 Update Cycle

There is no fixed calendar for updates. Updates are published when methodology or alignment changes justify a new version. Users should check the current version when comparing scores or commissioning assessments.

12.4 External Review Possibilities

The publisher may seek external review (academic, industry, or standards body) for major versions. Such review does not constitute formal endorsement. Any review process and outcomes are documented transparently.

12.5 Transparency Commitments

The publisher commits to: (1) documenting the control set, weights, and aggregation for each version; (2) stating assumptions and limitations clearly; (3) publishing version history and release notes; (4) not implying certification or endorsement where none exists.

13. Comparative Positioning

13.1 Differences from Generic Cyber Maturity Models

Generic cybersecurity maturity models (e.g., broad NIST CSF-based models) address a wide range of controls. The PQMM is focused exclusively on post-quantum readiness and related governance, inventory, infrastructure, transition, and awareness. It does not replace a general maturity assessment; it complements it with a PQC-specific view.

13.2 Complementarity with Enterprise Risk Frameworks

The PQMM can be used alongside enterprise risk management (ERM) and operational risk frameworks. PQC risk can be recorded in risk registers and mapped to PQMM dimensions for assessment. The framework does not prescribe how ERM integrates PQC; it provides a structured way to assess readiness once scope is defined.

13.3 Non-Substitution Statement

The PQMM does not substitute for: (1) a formal cryptographic or security audit; (2) penetration testing or red-team exercises; (3) certification against ISO 27001, SOC 2, or similar; (4) legal or regulatory compliance verification; (5) vendor or product certification. It is a self-assessment and planning-support tool.

14. Implementation Guidance

14.1 Organizational Preparation

Before assessment: define the organizational scope (entity, division, or perimeter); ensure that respondents have access to policies, inventories, and roadmaps; decide whether Quick or Complete Mode is appropriate for the intended use; allocate time for data collection and validation.

14.2 Internal Stakeholder Engagement

Engage governance (e.g., CISO, risk), technical (e.g., infrastructure, development), and compliance stakeholders so that responses reflect the actual state. Single-respondent assessments may under- or over-state maturity if one function does not have full visibility.

14.3 Reporting to Executive Leadership

Present the QRI and level as a readiness snapshot; use dimension scores to highlight strengths and gaps; avoid claiming “compliance” or “security” based solely on the model; recommend periodic reassessment to track progress.

14.4 Integration with Enterprise Risk Management

Map PQMM dimensions to existing risk taxonomies; record PQC risk in the risk register with reference to PQMM level or dimension scores; use roadmap and control gaps to inform risk treatment plans; align reporting with ERM cycles.

15. Conclusion

15.1 Strategic Implications

Post-quantum cryptographic transition is a multi-year organizational challenge. A structured maturity framework supports prioritization, resource allocation, and communication. The PQMM provides a formal, reproducible basis for assessment and tracking, within the limits of a self-disclosure model.

15.2 Long-Term Governance Outlook

Governance of cryptographic risk will remain relevant as standards and threats evolve. Embedding PQC readiness into policy, risk, and architecture governance supports the organization's ability to adapt as NIST and regulators publish further guidance.

15.3 Continuous Adaptation Imperative

The framework will be updated as standardization and regulation evolve. Users should treat the PQMM as a living reference and align their assessments and roadmaps with the current version and with external developments.

16. Practical adoption steps

Organizations using the PQMM often progress through a sequence of phases. The following is a generic progression; timing and depth depend on context and resources.

Awareness and scope. Establish shared understanding of post-quantum risk and of the framework. Define the perimeter to be assessed (entity, division, or system boundary). Assign ownership and decide whether Quick or Complete Mode is appropriate for the first assessment.

Inventory and governance. Build or update the cryptographic inventory and governance artefacts (policies, risk register, accountability). Run a first PQMM assessment to obtain a baseline QRI and dimension scores. Use the results to identify the largest gaps.

Prioritization and pilot. Prioritize systems and assets for migration (e.g. by sensitivity, lifetime, and exposure). Plan and execute a limited pilot (e.g. one application or one key exchange path) to validate interoperability and operational impact. Refine the roadmap and resource estimates.

Rollout and monitoring. Scale migration according to the prioritized roadmap. Integrate PQC readiness into ongoing governance (risk, compliance, architecture). Re-run the PQMM assessment periodically to track progress and adjust plans.

This sequence is illustrative; organizations may combine or reorder steps to fit their constraints. The PQMM supports each phase by providing a consistent maturity view and a basis for reporting and prioritization.

Annex A – Glossary

Control: A discrete criterion or question used to evaluate one aspect of a dimension. Each control has a unique identifier (e.g., G01, C02) and is associated with a dimension, tag (Direct, Migration, Hygiene), and criticality (Critical, High, Medium, Low).

Crypto-agility: The ability to replace or add cryptographic primitives (algorithms, key sizes, protocols) without redesigning systems. In technical terms: systems expose cryptographic choices via configuration or pluggable modules (e.g. cipher suites, key agreement, signature algorithms) so that algorithm replacement does not require code or architecture changes. Crypto-agility is a prerequisite for incremental PQC migration. See Annex B.

Cryptographic Bill of Materials (CBOM): An inventory of cryptographic assets (certificates, keys, libraries, protocols) that may be affected by the transition to post-quantum cryptography.

Dimension: One of five axes of the PQMM: Governance, Cryptography, Infrastructure, Transition, Awareness. Each dimension is evaluated through a set of controls and contributes a weighted share to the QRI.

Harvest Now, Decrypt Later (HNDL): A threat model in which an adversary collects encrypted data or communications today and stores them for decryption when sufficient computing power (e.g. a cryptographically relevant quantum computer) or algorithmic advance becomes available. HNDL implies that data protected only by classical public-key cryptography may be at future risk; it drives prioritization of long-lived and high-sensitivity data in PQC migration. See Annex B.

Maturity level: One of five levels (0–4) derived from the QRI score band. Level 0 = Unaware; Level 1 = Initial Awareness; Level 2 = Structured Assessment; Level 3 = Managed Transition; Level 4 = Strategically Integrated.

Post-quantum cryptography (PQC): Cryptographic algorithms designed to resist attacks from both classical and quantum computers. In this document, PQC refers in particular to algorithms standardized by NIST in 2024: ML-KEM (key encapsulation, FIPS 203), ML-

DSA (module-lattice signatures, FIPS 204), and SLH-DSA (hash-based signatures, FIPS 205), or equivalent international standards. See Annex B for PQC algorithm categories.

Post-quantum readiness: In this framework, the extent to which an organization has put in place governance, inventory, infrastructure, transition planning, and awareness necessary to make informed decisions about PQC adoption and to execute a controlled migration. See Section 2.1.

Quantum Readiness Index (QRI): A numerical score from 0 to 100, computed as the weighted sum of the five dimension scores. The QRI determines the maturity level.

Quick Mode: Assessment mode that evaluates a defined set of essential controls (e.g., 33) with binary scoring only. Used for baseline and periodic monitoring.

Complete Mode: Assessment mode that evaluates the full control set (e.g., 92 controls) with binary and, where applicable, text-quality scoring. Used for detailed migration planning and compliance preparation.

Annex B – Formal Definitions of Key Concepts

Post-Quantum Cryptography (PQC): Cryptographic mechanisms that remain secure against attacks using large-scale quantum computers. In practice, the term refers to algorithms standardized by NIST in 2024 (ML-KEM, ML-DSA, SLH-DSA in FIPS 203, 204, 205) or equivalent international standards. PQC may be deployed in hybrid mode alongside classical algorithms during transition. **PQC algorithm categories (NIST 2024):** (1) **Key encapsulation:** ML-KEM (FIPS 203), lattice-based; (2) **Digital signatures — module-lattice:** ML-DSA (FIPS 204); (3) **Digital signatures — hash-based:** SLH-DSA (FIPS 205). These categories cover the main functions (key agreement, signatures) required for migration; selection and combination depend on use case and standardization updates.

Crypto-Agility: The property of a system or organization that allows cryptographic primitives (algorithms, key lengths, protocols) to be updated or replaced without major redesign or redeployment. Technically this implies: centralized or parameterized choice of algorithms (e.g. TLS cipher suites, signature schemes), key management that supports algorithm rotation, and upgrade paths (e.g. OTA, config-driven) where applicable. Crypto-agility supports incremental migration to PQC and adaptation to future standard changes.

Harvest Now, Decrypt Later (HNDL): A threat model in which an attacker captures encrypted data or communications today and stores them for decryption when sufficient computing power (e.g. a cryptographically relevant quantum computer) or algorithmic advance becomes available. HNDL motivates prioritization of long-lived or high-value

secrets for PQC migration. Time-sensitive or short-retention data may be lower priority than data with long confidentiality horizons.

Hybrid Cryptographic Schemes: Combined use of a classical algorithm and a PQC algorithm for the same function (e.g. key exchange or signature) so that security depends on both. Hybrid schemes are used during transition to preserve security if one mechanism is broken.

Annex C – Normative References

The following standards and guidance are referenced in this framework. Titles, editions and years are given for citation; users should confirm the current versions when quoting. The list does not imply endorsement or certification by the publisher.

NIST Post-Quantum Cryptography (2024)

- FIPS 203: *Module-Lattice-Based Key-Encapsulation Mechanism Standard* (ML-KEM). NIST, 2024.
- FIPS 204: *Module-Lattice-Based Digital Signature Standard* (ML-DSA). NIST, 2024.
- FIPS 205: *Stateless Hash-Based Digital Signature Standard* (SLH-DSA). NIST, 2024.
- NIST CSRC Post-Quantum Cryptography: https://csrc.nist.gov/projects/post-quantum-cryptography

ISO/IEC

- ISO/IEC 27001:2022, *Information security management systems — Requirements* (including control A.10: Cryptography).
- ISO/IEC 27002:2022, *Security controls — Information security controls* (e.g. Clause 8.24 Cryptographic controls, 8.25 Secure development).

European Union

- Directive (EU) 2022/2555 (NIS2) on measures for a high common level of cybersecurity.
- Regulation (EU) 2022/2554 (DORA) on digital operational resilience for the financial sector.

National / agency guidance

- ANSSI: *Avis de l'ANSSI sur la migration vers la cryptographie post-quantique* (2023–2024). French national authority guidance on PQC migration. https://cyber.gouv.fr

Other

- ENISA publications on post-quantum cryptography.
- ETSI Quantum-Safe Cryptography: https://www.etsi.org/technologies/quantum-safe-cryptography

Annex D – Example Radar Visualization Template

A radar (spider) chart may be used to display the five dimension scores on a single plot. Each axis represents one dimension (Governance, Cryptography, Infrastructure, Transition, Awareness). The score for each dimension (0–100) is plotted on the corresponding axis; points are connected to form a polygon. This allows visual comparison of balance across dimensions. The same scale (0–100) should be used for all axes. The global QRI is not directly represented on the radar; it is the weighted sum of the five dimension values.

Methodological figures. The assessment flow can be summarized as: *Controls (per dimension) → dimension score (0–100) → weighted aggregation → QRI (0–100) → maturity level (0–4).* A diagram of this flow, and an example radar chart with dimension scores, are available in the Qubixor interactive demo at https://qubixor.com/demo (report and benchmark views). These illustrate the shape of the deliverable without prescribing a specific tool.

Annex E – Example Executive Reporting Template

Suggested structure for a one-page executive summary of PQMM results:

1. **Scope:** Organization or perimeter assessed; assessment date; framework version and mode (Quick/Complete).
2. **Overall result:** QRI score (0–100); maturity level (0–4) with short label.
3. **Dimension summary:** Table or radar with five dimension scores; highlight lowest dimension(s).
4. **Key gaps:** Up to three priority gaps derived from control-level results (no inference beyond what the model assesses).
5. **Next steps:** Recommended actions (e.g., build inventory, formalize roadmap, assign ownership).
6. **Caveats:** The assessment is based on self-disclosure; it does not constitute an audit or compliance attestation.

Example deliverable. A live example of the PQMM report format—including the QRI score, dimension radar, synthesis, and priority actions—is available in the Qubixor interactive

demo at https://qubixor.com/demo. The demo shows how the framework output is presented in practice (maturity report, benchmark comparison, ecosystem view) without implying a specific tool or vendor choice.
