QUBIXOR

Qubixor Post-Quantum Maturity Model (QPQMM)

Cadre méthodologique — Version 1.0

Février 2026

Qubixor

qubixor.com

Table des matières

Qubixor Post-Quantum Maturity Model (PQMM)

Cadre méthodologique – Version 1.0

Type de document : Cadre méthodologique
Version : 1.0
Date de publication : Février 2026
Éditeur : Qubixor

Résumé

Ce document définit le Qubixor Post-Quantum Maturity Model (PQMM), un cadre structuré pour évaluer la préparation des organisations à la transition vers la cryptographie post-quantique (PQC). Le cadre vise à soutenir les décisions de gouvernance et de gestion des risques en fournissant une évaluation de maturité reproductible et multidimensionnelle, alignée sur les thèmes de normalisation et de régulation largement reconnus. Le PQMM ne constitue pas un schéma de certification, un audit des implémentations cryptographiques ni une garantie de conformité à une réglementation donnée. Le document précise les fondements conceptuels du modèle, ses cinq dimensions (Gouvernance, Cryptographie, Infrastructure, Transition, Sensibilisation), une échelle de maturité à cinq niveaux, une méthodologie de notation pondérée produisant un Indice de préparation quantique (QRI), ainsi que les hypothèses et limites régissant l'usage du modèle. Il s'adresse aux responsables sécurité et risque, aux fonctions conformité et à la direction générale qui ont besoin d'une référence formelle et citável pour les discussions sur la préparation post-quantique. Le cadre est sectoriellement neutre et repose sur l'auto-déclaration des organisations ; son applicabilité aux environnements très classifiés ou restreints n'est pas supposée sans adaptation.

Résumé exécutif

1. Objectif du PQMM

Le PQMM fournit une méthode structurée et reproductible pour évaluer la posture d'une organisation vis-à-vis de la transition cryptographique post-quantique. Son objectif est de soutenir la gouvernance interne, la priorisation des risques et la communication avec les parties prenantes en cartographiant les pratiques et contrôles organisationnels sur une échelle de maturité définie et un indice numérique (QRI). Le cadre ne vise pas à remplacer les audits cryptographiques, les tests d'intrusion ou les évaluations formelles de conformité.

2. Pourquoi la préparation post-quantique exige un cadre structuré

Le passage de la cryptographie à clé publique actuelle aux algorithmes résistants aux ordinateurs quantiques implique des dimensions techniques, organisationnelles et de gouvernance. Sans modèle structuré, les organisations manquent d'un langage commun et d'une base cohérente pour mesurer les progrès. Un cadre de maturité permet des comparaisons dans le temps et soutient l'allocation des ressources et le reporting sans imposer un seul « chemin » de migration.

3. Ce que mesure le PQMM

Le PQMM mesure la présence et la maturité des éléments de gouvernance, de processus et de planification qui soutiennent la préparation post-quantique. Il évalue : (1) la gouvernance et la politique ; (2) l'inventaire cryptographique et la résilience ; (3) l'infrastructure et la préparation des fournisseurs ; (4) la planification de la transition et les dépendances ; (5) la sensibilisation et la formation. Chaque dimension est évaluée via un ensemble défini de contrôles ; les résultats au niveau des contrôles sont agrégés par dimension puis combinés en un indice unique, le Quantum Readiness Index (QRI), sur une échelle 0–100, mappé sur cinq niveaux de maturité.

4. Ce que le PQMM ne mesure pas

Le PQMM ne mesure pas la solidité cryptographique des systèmes déployés, l'exactitude des implémentations ni l'efficacité des contrôles techniques. Il ne certifie pas la conformité à une réglementation ou norme donnée. Il n'évalue pas les capacités de calcul quantique ni le calendrier des menaces quantiques. Les conclusions sur le risque résiduel ou l'adéquation à un cas d'usage particulier nécessitent une analyse complémentaire au-delà du modèle.

5. Public visé

Le document s'adresse aux : responsables sécurité et risque en charge de la stratégie PQC ; fonctions conformité et audit se préparant aux attentes réglementaires ; équipes IT et infrastructure impliquées dans l'inventaire cryptographique et la planification de la migration ; direction générale ayant besoin d'une référence formelle et neutre pour la communication conseil ou régulateur.

6. Composants structurels clés du modèle

Le modèle comprend : (1) cinq dimensions avec périmètre et unités d'évaluation explicites ; (2) un ensemble de contrôles (essentiels et complets) utilisé pour noter chaque dimension ; (3) un Quantum Readiness Index (QRI) 0–100 avec une formule d'agrégation et des pondérations par dimension définies ; (4) cinq niveaux de maturité (0–4) avec des caractéristiques observables ; (5) deux modes d'évaluation (Rapide et Complet) différant par

la couverture des contrôles et la granularité de la notation. Le versionnage, les hypothèses et les limites sont documentés dans le cadre.

1. Introduction

1.1 Contexte : transition cryptographique post-quantique

La cryptographie à clé publique actuellement déployée (ex. RSA, ECDH, ECDSA) est vulnérable aux attaques utilisant des ordinateurs quantiques suffisamment puissants. Les organismes de normalisation ont publié ou publient des normes de cryptographie post-quantique (ex. NIST FIPS 203, 204, 205). Les organisations qui dépendent de la confidentialité ou de l'intégrité des données à long terme peuvent avoir à planifier l'adoption de ces algorithmes. La transition touche la politique, l'inventaire, l'infrastructure, la planification et la sensibilisation ; ce n'est pas uniquement une mise à jour technique.

1.2 Paysage stratégique des risques

Les risques incluent : l'exposition des données actuellement chiffrées si elles sont collectées et déchiffrées plus tard (Harvest Now, Decrypt Later) ; l'incapacité à satisfaire les exigences réglementaires ou contractuelles futures ; et les perturbations opérationnelles si la migration est retardée jusqu'à l'obligation. Le PQMM ne quantifie pas ces risques ; il évalue les structures et processus organisationnels qui soutiennent la prise de décision éclairée et la préparation à la migration.

1.3 Besoin d'un modèle de maturité structuré

Les modèles de maturité sont utilisés en cybersécurité et en gestion des risques pour comparer les organisations, suivre les progrès et aligner les parties prenantes. Un modèle structuré pour la préparation post-quantique fournit une référence commune, réduit l'ambiguïté du reporting et soutient la priorisation. Le PQMM est conçu pour être reproductible (mêmes entrées, mêmes sorties) et pour séparer la maturité de gouvernance de l'exposition cryptographique technique lorsque c'est possible.

1.4 Périmètre et limites du document

Ce document définit la méthodologie du PQMM : dimensions, contrôles, notation, niveaux de maturité, interprétation et limites. Il ne prescrit pas de calendriers de migration, de choix de produits ni de stratégies de conformité. Le périmètre est la préparation organisationnelle telle qu'attestée par les politiques, inventaires, feuilles de route et sensibilisation ; il exclut la vérification directe des implémentations cryptographiques. Les réglementations

géographiques et sectorielles ne sont référencées qu'en termes généraux sauf citation explicite.

2. Fondements conceptuels

2.1 Définition de la préparation post-quantique

La préparation post-quantique (dans ce cadre) désigne la mesure dans laquelle une organisation a mis en place la gouvernance, l'inventaire, l'infrastructure, la planification de la transition et la sensibilisation nécessaires pour prendre des décisions éclairées sur l'adoption des normes cryptographiques post-quantiques et pour exécuter une migration maîtrisée lorsque le choix est fait. La préparation est donc une fonction de la maturité organisationnelle, et non de la solidité cryptographique actuelle d'un système donné.

2.2 Gouvernance vs exposition technique

Le PQMM distingue :

- **Maturité de gouvernance :** Existence et clarté des politiques, responsabilités (ex. RACI), registres de risques, budgets et veille réglementaire. C'est évalué principalement dans la dimension Gouvernance et reflété dans les autres dimensions où la responsabilité et le processus sont évalués.
- **Exposition technique :** L'usage réel d'algorithmes vulnérables, de longueurs de clé ou de protocoles. Le PQMM ne mesure pas directement l'exposition technique ; il évalue si l'organisation dispose d'un inventaire, d'une classification et de feuilles de route permettant une analyse d'exposition.

Un score de gouvernance élevé n'implique pas une exposition technique faible ; un score de gouvernance faible n'implique pas une exposition élevée. Les deux vues sont complémentaires.

2.3 La crypto-agilité comme principe fondateur

La crypto-agilité (voir Annexe B) est la capacité à remplacer ou ajouter des primitives cryptographiques sans repenser les systèmes. Le PQMM traite la crypto-agilité comme un facilitateur d'une migration PQC maîtrisée et l'évalue dans les dimensions Cryptographie et Infrastructure (ex. gestion centralisée des chiffrements, architecture de gestion des clés, évolutivité). Les niveaux de maturité 3 et au-delà supposent des progrès mesurables vers une conception crypto-agile.

2.4 Hypothèses sur l'horizon de risque

Le modèle suppose que les organisations planifient sur un horizon pluriannuel et que la normalisation (ex. NIST) et les orientations réglementaires continueront d'évoluer. Il ne suppose pas de date précise à laquelle les menaces quantiques se matérialiseront ni à laquelle la migration devra être terminée. Les hypothèses temporelles dans la notation (ex. présence d'une feuille de route jalonnée) reflètent la maturité de la planification, et non une échéance fixe.

2.5 Principes de conception du modèle

1. **Neutralité :** Le cadre ne favorise aucun fournisseur, produit ou stratégie de migration. Les contrôles sont exprimés en termes de résultats et d'artefacts, non de technologies.
2. **Reproductibilité :** Le même ensemble de réponses, pour un même mode d'évaluation et une même version, produit le même QRI et le même niveau de maturité.
3. **Scalabilité :** La même structure s'applique à des organisations de tailles et secteurs différents ; l'applicabilité des contrôles peut être interprétée selon le contexte sans modifier la logique de notation.
4. **Conception sectoriellement neutre :** Aucune dimension ni aucun contrôle n'est défini exclusivement pour un seul secteur. Les orientations sectorielles sont fournies séparément (Section 9) sous forme de notes d'application, et non dans le cadre du scoring central.

3. Alignement normatif et standards

3.1 Alignement avec la normalisation post-quantique NIST

Le PQMM utilise la normalisation post-quantique NIST comme référence technique pour ce que « post-quantique » et « résistant au quantique » signifient en pratique. Concrètement, le cadre suppose que l'adoption ou l'adoption planifiée de mécanismes tels que ceux spécifiés dans FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) et FIPS 205 (SLH-DSA), ou d'algorithmes standardisés équivalents, constitue l'état cible. Le modèle ne certifie pas la conformité aux normes NIST ; il évalue si l'organisation a une gouvernance, un inventaire et des feuilles de route orientés vers une telle adoption.

3.2 Alignement avec les standards de gouvernance cryptographique

La gouvernance cryptographique est abordée dans des normes internationales telles qu'ISO/CEI 27001 et ISO/CEI 27002 (contrôles cryptographiques). La dimension Gouvernance du PQMM recoupe conceptuellement les objectifs de contrôle liés à la

politique, à l'évaluation des risques et à la gestion des actifs. Le cadre ne prétend pas couvrir tous les contrôles ISO 27001/27002 ; il se concentre sur ceux pertinents pour la planification et la migration post-quantiques.

3.3 Relation avec les contrôles cryptographiques ISO 27001 / 27002

L'ISO/CEI 27002 inclut des contrôles pour la gestion des clés cryptographiques, l'usage de la cryptographie et le développement sécurisé. Les dimensions du PQMM (notamment Cryptographie et Infrastructure) traitent des thèmes similaires dans le contexte de la transition PQC. L'alignement est au niveau des objectifs de contrôle (ex. inventaire, politique, gestion des clés), et non d'une correspondance contrôle à contrôle. L'usage du PQMM ne se substitue pas à une certification ISO 27001 ou à une analyse d'écart.

3.4 Complémentarité avec les cadres de cybersécurité existants

Le PQMM vise à compléter, et non à remplacer, les cadres de risque et de sécurité existants (ex. NIST Cybersecurity Framework, cadres sectoriels). Les organisations peuvent mapper les dimensions du PQMM à leurs ensembles de contrôles pour le reporting ; le cadre n'exige pas l'adoption d'un cadre global particulier.

3.5 Tableau de correspondance normative

Le tableau suivant indique la nature de l'alignement entre les dimensions du PQMM et des thèmes normatifs sélectionnés. « Direct » indique un recouvrement clair de périmètre ; « Partiel » indique un recouvrement partiel ou une dépendance à l'interprétation ; « Complémentaire » indique que le PQMM apporte un angle spécifique PQC à un thème plus large. Le tableau intègre les normes post-quantiques NIST finalisées en 2024 (FIPS 203 ML-KEM, FIPS 204 ML-DSA, FIPS 205 SLH-DSA) et les orientations européennes/nationales (ex. avis ANSSI sur la migration).

Dimension PQMM	NIST PQC (FIPS 203/204/205, 2024)	ISO 27001/27002 (crypto)	Thèmes type NIS2/DORA	ANSSI / orientations nationales PQC
Gouvernance	Partiel (planification migration)	Partiel	Direct (gouvernance, risque, reporting)	Partiel (stratégie, responsabilité)
Cryptographie	Direct (adoption algorithmes, inventaire)	Direct	Partiel	Direct (recommandations, migration)

Dimension PQMM	NIST PQC (FIPS 203/204/205, 2024)	ISO 27001/27002 (crypto)	Thèmes type NIS2/DORA	ANSSI / orientations nationales PQC
Infrastructure	Partiel (déploiement, évolutivité)	Partiel	Partiel	Partiel (préparation infrastructure)
Transition	Direct (feuille de route, déploiement hybride)	Complémentaire	Partiel	Direct (phases de migration)
Sensibilisation	Complémentaire	Complémentaire	Partiel	Complémentaire

Ce tableau est à titre de référence conceptuelle uniquement. Il n'implique pas d'aval formel d'un organisme de normalisation ou d'un régulateur. Pour les références normatives précises, voir l'Annexe C.

Indépendance intellectuelle. Le PQMM est un cadre méthodologique indépendant développé par Qubixor. Il ne représente pas la position officielle d'aucune autorité gouvernementale ou réglementaire. Les références à NIST, ANSSI, ENISA, NIS2, DORA ou d'autres organismes indiquent un alignement sur les thèmes ou normes que ces entités publient ; elles n'impliquent pas leur aval.

4. Architecture du modèle

4.1 Vue d'ensemble structurelle

Le PQMM comprend cinq dimensions. Chaque dimension est évaluée via un ensemble de contrôles. Les scores au niveau des contrôles sont agrégés pour produire un score de dimension ; les scores des dimensions sont combinés à l'aide de pondérations fixes pour produire l'Indice de préparation quantique (QRI). Le QRI est mappé sur l'un des cinq niveaux de maturité. Deux modes d'évaluation sont définis : Mode rapide (contrôles essentiels uniquement) et Mode complet (ensemble complet de contrôles), avec des règles d'agrégation cohérentes.

Flux de notation (visuels méthodologiques) : Un schéma simple peut représenter le flux : *Contrôles (par dimension) → score de dimension (0–100) → somme pondérée → QRI (0–100) → niveau de maturité (0–4).* Les cinq dimensions constituent les entrées de l'agrégation ; le graphique radar (Annexe D) est la représentation usuelle des scores par dimension aux côtés du QRI unique.

4.2 Dimensions du PQMM

4.2.1 Gouvernance

4.2.1.1 Définition formelle

La dimension Gouvernance évalue la mesure dans laquelle l'organisation a défini les responsabilités, la politique, la gestion des risques et l'allocation des ressources pour la transition cryptographique post-quantique. Elle traite de la présence et de la clarté des structures et processus permettant une prise de décision et une supervision éclairées.

4.2.1.2 Périmètre

Structures organisationnelles, mécanismes de responsabilité (ex. RACI), supervision stratégique, registres de risques, budget et parrainage, veille réglementaire et normative liée à la PQC.

4.2.1.3 Inclusions explicites

Politique formelle de cryptographie ou de sécurité de l'information ; registre de risques post-quantique ou HNDL avec responsables identifiés ; RACI ou équivalent pour la cryptographie, la PKI et la gestion des clés ; classification des données incluant l'horizon de confidentialité ; budget dédié ou alloué aux initiatives PQC ; veille réglementaire et normative (ex. NIST, ENISA, mapping sectoriel).

4.2.1.4 Exclusions explicites

Détails opérationnels d'implémentation de la cryptographie ; conception technique des systèmes de gestion des clés ; sélection de fournisseurs ou évaluation de produits.

4.2.1.5 Unité d'évaluation

La dimension est évaluée au niveau de l'organisation (ou du périmètre défini). L'unité d'évaluation est la présence et la maturité des artefacts de gouvernance et des responsabilités assignées, et non l'exactitude technique des implémentations cryptographiques.

4.2.2 Cryptographie

4.2.2.1 Définition formelle

La dimension Cryptographie évalue l'inventaire des actifs cryptographiques de l'organisation, la classification des données par horizon de confidentialité, les politiques TLS et de gestion des clés, et les progrès vers un déploiement post-quantique ou hybride (ex. pilotes, feuilles de route).

4.2.2.2 Périmètre

Inventaire cryptographique (style CBOM) ; classification des données par sensibilité et horizon ; politique TLS et gestion des chiffrements ; architecture de gestion des clés (KMS/HSM) ; feuille de route et pilotes post-quantiques ou hybrides ; stratégie d'archivage et de protection à long terme.

4.2.2.3 Inclusions explicites

Inventaire cryptographique centralisé ou consolidé avec couverture définie ; classification des données par horizon de confidentialité ; politique TLS formalisée et appliquée ; feuille de route pour l'adoption TLS/KEM hybride ou PQC avec jalons ; gestion centralisée des clés ; pilotes PQC utilisant des algorithmes standardisés ; stratégie de protection cryptographique à long terme des données archivées.

4.2.2.4 Exclusions explicites

Choix de produits spécifiques aux fournisseurs ; conception d'algorithmes cryptographiques ; vérification formelle des implémentations.

4.2.2.5 Unité d'évaluation

La dimension est évaluée au niveau de la gouvernance et de la planification cryptographiques de l'organisation. L'unité est l'existence et la maturité des artefacts d'inventaire, de politique et de feuille de route, et non la solidité cryptographique de chaque actif.

4.2.3 Infrastructure

4.2.3.1 Définition formelle

La dimension Infrastructure évalue la mesure dans laquelle les systèmes et les relations avec les fournisseurs soutiennent l'évolutivité cryptographique, une gestion TLS et des certificats cohérente, et l'alignement avec les feuilles de route PQC (ex. KMS/HSM cloud, évolutivité OTA).

4.2.3.2 Périmètre

Terminaison TLS et gestion des chiffrements ; inventaire des certificats et des clés sur l'infrastructure ; gestion des clés cloud et sur site avec feuille de route PQC ; évolutivité cryptographique over-the-air ou équivalent ; profils VPN et crypto réseau ; cycle de vie des certificats et surveillance d'épuisement.

4.2.3.3 Inclusions explicites

Architecture de terminaison TLS cohérente ; gestion centralisée des chiffrements (ex. via IaC) ; inventaire des certificats sur les systèmes dans le périmètre ; KMS/HSM cloud avec feuille de route PQC documentée ; évolutivité crypto OTA ou équivalent le cas échéant ;

profils VPN et associés alignés sur hybride/PQC ; surveillance de l'expiration et de l'épuisement des certificats.

4.2.3.4 Exclusions explicites

Topologie réseau détaillée ; planification des performances ou de la capacité ; détails d'implémentation spécifiques aux fournisseurs au-delà de la feuille de route et des capacités.

4.2.3.5 Unité d'évaluation

La dimension est évaluée au niveau de la gouvernance d'infrastructure et des capacités documentées de l'organisation. L'unité est la présence et la maturité des artefacts architecturaux et opérationnels permettant la migration PQC.

4.2.4 Transition

4.2.4.1 Définition formelle

La dimension Transition évalue la présence et la qualité des feuilles de route de migration, la priorisation (ex. par risque HNDL), la stratégie de déploiement hybride et les tests de performance ou d'intégration liés à la PQC.

4.2.4.2 Périmètre

Feuille de route de migration PQC jalonnée ; critères de priorisation (ex. exposition HNDL, criticité) ; approche de déploiement hybride par domaine ou type de système ; tests de performance et de compatibilité ; stratégie de déploiement par phases.

4.2.4.3 Inclusions explicites

Feuille de route PQC documentée avec jalons ; priorisation de la migration par risque ou impact métier ; stratégie de déploiement hybride par domaine ; tests de performance ou de compatibilité KEM/signature ; plan de déploiement hybride par phases.

4.2.4.4 Exclusions explicites

Calendriers de projet exacts (sauf utilisés uniquement comme preuve de maturité de planification) ; feuilles de route fournisseurs ; étapes techniques détaillées de migration.

4.2.4.5 Unité d'évaluation

La dimension est évaluée au niveau de la planification de la transition de l'organisation. L'unité est l'existence et la clarté des artefacts de feuille de route, priorisation et déploiement.

4.2.5 Sensibilisation

4.2.5.1 Définition formelle

La dimension Sensibilisation évalue la mesure dans laquelle l'organisation a mis en place des briefings dirigeants, des formations techniques et un engagement externe liés à la cryptographie post-quantique et au risque quantique.

4.2.5.2 Périmètre

Sensibilisation au niveau dirigeant au risque quantique et PQC ; formation technique sur la PQC pour les rôles concernés ; participation à des initiatives sectorielles ou de normalisation.

4.2.5.3 Inclusions explicites

Briefings dirigeants sur le risque quantique et la PQC ; programmes ou supports de formation technique PQC ; engagement externe (ex. forums, participation à la normalisation, partage d'information).

4.2.5.4 Exclusions explicites

Profondeur ou qualité des connaissances techniques ; certification des personnes ; contenu marketing ou de communication externe.

4.2.5.5 Unité d'évaluation

La dimension est évaluée au niveau de l'organisation. L'unité est la présence des activités de briefing, formation et engagement, et non la compétence mesurée des individus.

5. Cadre des niveaux de maturité

5.1 Vue d'ensemble de la structure des niveaux

Le PQMM définit cinq niveaux de maturité, numérotés de 0 à 4. Chaque niveau correspond à une bande de score QRI. Le niveau est déterminé uniquement par la valeur du QRI ; il n'y a pas de dépassement qualitatif séparé. Les bandes sont : Niveau 0 (QRI 0–20) ; Niveau 1 (20–40) ; Niveau 2 (40–60) ; Niveau 3 (60–80) ; Niveau 4 (80–100).

5.2 Niveau 0 – Non conscient / Non structuré

Caractéristiques organisationnelles : Aucune reconnaissance formelle du risque post-quantique au niveau dirigeant ; aucune responsabilité dédiée pour la cryptographie ou la PQC ; aucune considération de calendrier ou de feuille de route.

Posture de gouvernance : Aucune politique cryptographique ne faisant référence à la PQC ou au risque quantique ; aucune entrée de registre de risques pour HNDL ou PQC ; aucun responsable assigné pour les décisions cryptographiques ou de gestion des clés.

Maturité de l'inventaire cryptographique : Aucun inventaire cryptographique centralisé ; aucune classification systématique des données par horizon de confidentialité.

Profil de risque résiduel : L'organisation n'a pas évalué l'exposition ; aucune base de priorisation. L'exposition résiduelle est indéfinie du point de vue du modèle.

Indicateurs observables : Absence de politique, registre de risques, RACI et artefacts d'inventaire ; aucune preuve de briefing dirigeant ou de budget PQC.

5.3 Niveau 1 – Sensibilisation initiale

Caractéristiques organisationnelles : Sensibilisation générale au risque post-quantique ; suivi des développements NIST ou de l'écosystème ; pas d'évaluation organisationnelle structurée ni de feuille de route formelle.

Posture de gouvernance : Une certaine sensibilisation au niveau dirigeant ; discussions de risque possibles ad hoc ; pas de politique ni de RACI formels ; pas de budget dédié.

Maturité de l'inventaire cryptographique : Pas d'inventaire complet ; éventuellement des listes partielles ou informelles ; pas de classification formelle des données par horizon.

Profil de risque résiduel : Le risque est reconnu mais pas cartographié de manière systématique ; la priorisation n'est pas possible sur une base structurée.

Indicateurs observables : Preuve de veille (ex. participation à des événements, lecture) ; pas de politique formelle, pas de feuille de route jalonnée, pas de CBOM.

5.4 Niveau 2 – Évaluation structurée

Caractéristiques organisationnelles : Inventaire cryptographique (CBOM) initié ; cartographie des risques réalisée ; visibilité dirigeante sur la PQC ; responsabilité définie pour au moins certains domaines cryptographiques.

Posture de gouvernance : Politique ou registre de risques documenté faisant référence à la PQC ; RACI ou équivalent pour crypto/PKI/KMS ; classification des données incluant l'horizon ; budget ou parrainage.

Maturité de l'inventaire cryptographique : Inventaire couvrant un périmètre défini ; politique TLS documentée ; feuille de route pouvant exister mais pas encore détaillée ou jalonnée.

Profil de risque résiduel : L'organisation peut identifier les actifs critiques et les zones à forte exposition ; la priorisation est possible ; la migration n'est pas encore planifiée de manière

systématique.

Indicateurs observables : Existence de CBOM, d'entrées de registre de risques, de RACI, de classification des données ; briefing dirigeant ou visibilité au conseil ; pas encore de crypto-agilité complète ni de migration maîtrisée.

5.5 Niveau 3 – Transition maîtrisée

Caractéristiques organisationnelles : Stratégie de migration rédigée ; gouvernance définie et maintenue ; crypto-agilité en place ou en cours (capacité à changer les primitives sans refonte complète).

Posture de gouvernance : Politique, registre de risques et RACI maintenus ; veille réglementaire et normative ; risque PQC quantifié le cas échéant ; budget et parrainage clairs.

Maturité de l'inventaire cryptographique : Inventaire à couverture élevée ; politiques TLS et KMS appliquées ; pilotes hybrides ou PQC en cours ; feuille de route avec jalons.

Profil de risque résiduel : Parcours de migration priorisé ; l'exposition résiduelle est comprise et gérée dans la feuille de route ; la crypto-agilité réduit le lock-in.

Indicateurs observables : Feuille de route jalonnée ; stratégie de déploiement hybride ; gestion centralisée des chiffrements/clés ; pilotes PQC ; conception crypto-agile dans les systèmes critiques.

5.6 Niveau 4 – Intégration stratégique

Caractéristiques organisationnelles : Feuille de route alignée sur les calendriers de normalisation ; architecture crypto-agile là où c'est critique ; fournisseurs et écosystème passés en revue ; capacités intégrées aux cycles de gouvernance et de planification.

Posture de gouvernance : PQC intégrée dans le risque et la stratégie ; revue régulière de la feuille de route et du risque ; responsabilité et budget complets ; engagement externe et alignement sur les standards.

Maturité de l'inventaire cryptographique : Inventaire complet ; adoption hybride ou PQC dans les chemins critiques ; stratégie d'archivage définie ; surveillance continue du cycle de vie des certificats et des clés.

Profil de risque résiduel : Migration en cours ou planifiée avec responsabilité claire ; exposition résiduelle consciemment acceptée ou atténuée ; l'organisation est prête à s'adapter à l'évolution des standards.

Indicateurs observables : Alignement documenté avec les calendriers NIST ou équivalents ; crypto-agilité démontrée ; préparation PQC des fournisseurs évaluée ; processus de

surveillance et de mise à jour continus.

6. Méthodologie de notation

6.1 Définition de l'échelle de notation

La notation au niveau des contrôles est binaire (mis en œuvre / non mis en œuvre) en mode Rapide. En mode Complet, une partie du score peut refléter la qualité des réponses en texte libre (pertinence, clarté, spécificité) en plus du statut binaire de mise en œuvre. Les scores au niveau des dimensions sont normalisés sur une échelle commune (ex. 0–100 par dimension). Le QRI global est la somme pondérée des scores des dimensions, normalisée à 0–100.

Valeurs de score : Chaque contrôle contribue au score de sa dimension. L'agrégation utilise des pondérations de tag (ex. Direct 1,00, Migration 0,95, Hygiène 0,85) et des pondérations de criticité (ex. Critique 1,15, Élevé 1,00, Moyen 0,90, Faible 0,80) de sorte que les contrôles soient pondérés par pertinence et criticité. Les pondérations exactes sont définies dans la configuration d'évaluation et sont fixes pour une version donnée du cadre.

6.2 Logique de notation au niveau des dimensions

Au sein de chaque dimension, les scores des contrôles sont combinés par moyenne pondérée. Les pondérations reflètent le tag (Direct, Migration, Hygiène) et la criticité (Critique, Élevé, Moyen, Faible) assignés à chaque contrôle. Le résultat est un score de dimension sur la même échelle que le QRI global (0–100). Les contrôles manquants ou non applicables sont exclus du dénominateur pour cette dimension afin que le score de dimension reflète uniquement l'ensemble applicable.

6.3 Modèle de pondération

Les cinq dimensions ont les pondérations suivantes dans le QRI global : Gouvernance 18 % ; Cryptographie 24 % ; Infrastructure 20 % ; Transition 20 % ; Sensibilisation 18 %. Ces pondérations reflètent une hypothèse de conception selon laquelle l'inventaire cryptographique et la résilience (Cryptographie) et la préparation de l'infrastructure (Infrastructure, Transition) sont au cœur de la capacité de migration, tandis que la Gouvernance et la Sensibilisation sont des facilitateurs. Les pondérations sont fixes pour la version du cadre et ne sont pas ajustées par organisation ou secteur.

6.4 Formule d'agrégation

Soit (d_1, \ldots, d_5) les scores des dimensions (chacun entre 0 et 100) pour Gouvernance, Cryptographie, Infrastructure, Transition et Sensibilisation respectivement. Soit (w_1 = 0{,}18), (w_2 = 0{,}24), (w_3 = 0{,}20), (w_4 = 0{,}20), (w_5 = 0{,}18). Alors :

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

Le QRI est donc dans l'intervalle 0–100. Le niveau de maturité est dérivé des bandes de QRI : 0–20 → Niveau 0 ; 20–40 → Niveau 1 ; 40–60 → Niveau 2 ; 60–80 → Niveau 3 ; 80–100 → Niveau 4.

6.5 Contrôles de cohérence

Le même mode d'évaluation (Rapide ou Complet) et la même version du cadre doivent être utilisés pour comparer les scores dans le temps ou entre organisations. Les ensembles de contrôles diffèrent selon les modes ; le QRI peut différer pour une même organisation entre les modes. La reproductibilité n'est assurée qu'au sein d'un seul mode et d'une seule version.

6.6 Considérations de sensibilité

De petits changements sur quelques contrôles peuvent déplacer le QRI de quelques points ; près d'une frontière (ex. 38–42), un petit changement peut modifier le niveau de maturité. Les utilisateurs doivent interpréter le niveau comme une bande, et non comme une classification précise. Les scores au niveau des dimensions apportent plus de nuance que le QRI unique.

7. Cadre d'interprétation

7.1 Interprétation du score global

Un QRI faible indique que l'organisation n'a pas encore mis en place les artefacts de gouvernance, d'inventaire et de planification que le modèle considère comme indicateurs de préparation. Il ne mesure pas directement l'exposition technique ni le risque résiduel. Un QRI élevé indique que l'organisation a documenté des politiques, inventaires, feuilles de route et activités de sensibilisation répondant aux critères des contrôles ; il ne certifie pas l'exactitude des implémentations ni la conformité à une réglementation.

7.2 Interprétation des déséquilibres entre dimensions

Un déséquilibre entre dimensions (ex. Cryptographie élevée, Gouvernance faible) suggère que les progrès techniques peuvent devancer la supervision et l'allocation des ressources,

ou inversement que la gouvernance existe sans inventaire ni feuille de route correspondants. Un tel déséquilibre n'implique pas qu'une dimension soit « plus importante » ; il indique où un focus supplémentaire peut être nécessaire pour une posture de préparation équilibrée.

7.3 Exposition au risque vs maturité organisationnelle

Le modèle ne produit pas de métrique d'exposition au risque. La maturité (et le QRI) reflète la maturité des processus et des artefacts, et non l'exposition réelle des actifs. Une organisation à maturité élevée peut encore avoir une exposition significative si la migration n'est pas encore exécutée ; une organisation à maturité faible peut avoir une exposition faible par hasard ou par périmètre. L'interprétation pour les décisions de risque doit combiner le résultat du PQMM avec une analyse d'exposition ou d'impact séparée.

7.4 Guide d'interprétation pour le conseil

Pour les conseils et la direction générale, le QRI et le niveau peuvent être présentés comme : (1) un instantané de la préparation organisationnelle tel que défini par le cadre ; (2) une base pour suivre les progrès dans le temps ; (3) une référence commune pour les discussions sur les ressources et les priorités. Le cadre ne permet pas de conclure que l'organisation est « sécurisée » ou « conforme » ; il permet de conclure que les éléments de gouvernance et de planification définis sont en place à un certain degré.

7.5 Interprétation technique vs stratégique

Les publics techniques peuvent utiliser le détail au niveau des dimensions et des contrôles pour identifier les écarts et planifier la remédiation. Les publics stratégiques peuvent utiliser le niveau global et le QRI pour le reporting et la comparaison. Le modèle ne permet pas de conclure sur l'efficacité de contrôles spécifiques ni sur l'adéquation de choix techniques spécifiques.

7.6 Exemples narratifs d'interprétation

Les scénarios suivants illustrent comment lire les scores en pratique :

- **QRI élevé mais une dimension nettement plus faible :** Par exemple, Cryptographie et Infrastructure sont solides (ex. 75–85) mais Sensibilisation à 35. Cela suggère que la préparation technique et infrastructure devance la sensibilisation et la formation. La priorité n'est pas d'ajouter des contrôles dans les dimensions fortes mais de combler l'écart de sensibilisation pour aligner les décisions et la communication avec la posture réelle.
- **Équilibre approximatif entre dimensions mais QRI dans la bande 40–50 :** L'organisation a une approche structurée dans les cinq dimensions mais n'a pas encore atteint la

transition maîtrisée (ex. pas de feuille de route jalonnée, pas de pilotes hybrides). Interprétation : la baseline est en place ; la prochaine étape est de passer de « nous savons ce que nous avons » à « nous avons un plan et nous l'exécutons », notamment en Transition et Cryptographie.

- **Gouvernance élevée, Cryptographie et Infrastructure plus faibles :** Les scores Gouvernance et Sensibilisation sont élevés (ex. 70+), mais Cryptographie et Infrastructure sont dans la fourchette 30–45. Cela indique que la politique et la responsabilité existent sans être encore étayées par un inventaire cryptographique mature, un alignement TLS/KMS ou une feuille de route infrastructure. Message pour la direction : la gouvernance est prête ; le goulot d'étranglement est l'exécution technique et l'inventaire—les ressources et priorités doivent s'y concentrer.

8. Cadre du parcours de migration

8.1 Modèle de transition par phases

Les phases suivantes décrivent une séquence logique pour construire la préparation. Ce ne sont pas des phases calendaires ; la durée dépend du contexte organisationnel.

Phase 0 – Sensibilisation

Objectifs : Établir la sensibilisation des dirigeants et des parties prenantes au risque post-quantique et à la nécessité d'une réponse structurée.

Artefacts requis : Preuve de briefing ou de formation ; attribution de responsabilité (même initiale).

Points de contrôle de gouvernance : Reconnaissance de la PQC dans les discussions risque ou stratégie.

Indicateurs de complétion : Activité de sensibilisation documentée ; responsable ou sponsor nommé.

Phase 1 – Inventaire cryptographique

Objectifs : Construire un inventaire des actifs cryptographiques (CBOM) et classifier les données par horizon de confidentialité pour permettre la priorisation.

Artefacts requis : Inventaire couvrant un périmètre défini ; politique ou matrice de classification des données incluant l'horizon.

Points de contrôle de gouvernance : Responsabilité de l'inventaire ; lien avec le registre de risques.

Indicateurs de complétion : Inventaire avec couverture définie ; classification appliquée aux données critiques.

Phase 2 – Mise en place de la crypto-agilité

Objectifs : Établir l'architecture et les processus permettant de mettre à jour les primitives cryptographiques sans refonte complète du système.

Artefacts requis : Gestion centralisée des chiffrements et des clés ; chemin de mise à jour documenté ; politique TLS et KMS.

Points de contrôle de gouvernance : Revue d'architecture ; alignement avec la feuille de route.

Indicateurs de complétion : Gestion centralisée en place ; évolutivité OTA ou équivalent le cas échéant.

Phase 3 – Migration maîtrisée

Objectifs : Exécuter un plan de migration priorisé en utilisant des mécanismes hybrides ou PQC conformes à la normalisation.

Artefacts requis : Feuille de route jalonnée ; stratégie de déploiement hybride ; résultats de pilotes ; tests de performance et de compatibilité.

Points de contrôle de gouvernance : Revue régulière de la feuille de route ; mises à jour du registre de risques ; budget et allocation des ressources.

Indicateurs de complétion : Pilotes terminés ; plan de déploiement pour les systèmes critiques ; surveillance en place.

Phase 4 – Surveillance continue

Objectifs : Intégrer la PQC dans la gouvernance continue, la gestion du cycle de vie et la gestion des fournisseurs.

Artefacts requis : Surveillance continue de l'inventaire et des certificats ; évaluation de la préparation PQC des fournisseurs ; mise à jour des politiques et feuilles de route à l'évolution des standards.

Points de contrôle de gouvernance : Intégration aux cycles risque et conformité ; engagement externe.

Indicateurs de complétion : Surveillance maintenue ; revue régulière de la feuille de route et du risque ; adaptation aux nouveaux standards.

9. Cadre d'application sectorielle

9.1 Secteur financier

Profil d'exposition typique : Forte dépendance à la cryptographie pour les transactions, l'identité et la protection des données ; attentes réglementaires (ex. DORA) sur le risque et la résilience TIC.

Complexité de gouvernance : Souvent élevée ; cadres de risque et de conformité existants ; nécessité de mapper le PQMM aux ensembles de contrôles réglementaires.

Contraintes de migration : Systèmes legacy ; dépendances tierces ; exigences de certification et d'audit.

Priorités spécifiques PQMM : Dimensions Gouvernance et Transition pour la feuille de route et l'alignement réglementaire ; Cryptographie et Infrastructure pour l'inventaire et la gestion des clés.

9.2 Infrastructure critique

Profil d'exposition typique : Technologie opérationnelle et systèmes à cycle de vie long ; exposition HNDL potentielle pour les données opérationnelles sensibles.

Complexité de gouvernance : Réglementations sectorielles (ex. NIS2) ; multiples parties prenantes ; contraintes de sécurité et de disponibilité.

Contraintes de migration : Cycles de mise à jour longs ; dépendance aux fournisseurs ; besoin de migration hybride ou progressive.

Priorités spécifiques PQMM : Transition et Infrastructure pour la feuille de route et l'évolutivité ; Gouvernance pour le registre de risques et la responsabilité.

9.3 Organisations du secteur public

Profil d'exposition typique : Données des citoyens et de l'État ; archivage à long terme ; conformité aux cadres nationaux et européens.

Complexité de gouvernance : Contraintes d'achat et de normalisation ; orientations nationales en cybersécurité (ex. ANSSI).

Contraintes de migration : Cycles budgétaires ; services centralisés ou partagés ; exigences de certification.

Priorités spécifiques PQMM : Gouvernance pour la politique et la veille réglementaire ; Cryptographie et Transition pour l'inventaire et l'alignement de la feuille de route avec les

calendriers nationaux.

9.4 Organisations SaaS et cloud-native

Profil d'exposition typique : Données clients dans le cloud ; TLS et sécurité des API ; dépendance aux capacités cryptographiques du fournisseur cloud.

Complexité de gouvernance : Variable ; peut être plus agile ; conformité (ex. SOC 2, sectorielle) possible.

Contraintes de migration : Dépendance à la feuille de route du fournisseur ; considérations multi-tenant ; frontières de gestion des clés.

Priorités spécifiques PQMM : Infrastructure et Cryptographie pour le fournisseur et la gestion des clés ; Transition pour l'alignement de la feuille de route avec le fournisseur et les standards.

10. Méthodologie de collecte et d'agrégation des données

10.1 Types de données collectées

L'évaluation PQMM collecte : (1) les réponses aux questions au niveau des contrôles (binaires et, en mode Complet, texte libre) ; (2) un contexte organisationnel optionnel (secteur, tranche de taille) pour le benchmarking ; (3) aucun accès direct aux systèmes ni au matériel cryptographique. Toutes les données sont fournies par l'organisation (auto-déclaration).

10.2 Principes d'anonymisation

Lorsque les données sont utilisées pour le benchmarking ou la recherche : les identifiants sont supprimés ou pseudonymisés ; l'agrégation est au niveau de groupe (ex. secteur, taille) ; aucune organisation n'est identifiable dans les benchmarks publiés. La participation au benchmarking peut être optionnelle.

10.3 Logique d'agrégation

Les agrégats de benchmark (ex. QRI médian par secteur) sont calculés à partir d'évaluations partageant la même version du cadre et le même mode d'évaluation. L'agrégation est descriptive (ex. médiane, quartiles) ; aucune inférence statistique sur la représentativité n'est faite sauf si explicitement indiqué et méthodologiquement documenté.

10.4 Limites statistiques

Les benchmarks dépendent de la population des organisations participantes. Ils ne sont pas nécessairement représentatifs d'un secteur ou d'une géographie. La taille d'échantillon et le biais de sélection ne sont pas contrôlés par le cadre. L'usage des benchmarks pour la comparaison est à la discrétion de l'utilisateur.

10.5 Méthode de construction des benchmarks

Lorsque des benchmarks sont publiés : la méthode de construction (population, filtres, agrégation, version, mode) est documentée. Les benchmarks sont mis à jour périodiquement ; la date et la méthode sont indiquées pour que les utilisateurs puissent évaluer la pertinence.

11. Hypothèses et limites du modèle

11.1 Hypothèses centrales

Le modèle suppose que : (1) les organisations peuvent et fourniront une auto-déclaration exacte ; (2) l'ensemble des contrôles et les pondérations reflètent une vision plausible de la préparation cohérente entre les évaluations ; (3) la normalisation (ex. NIST) et les thèmes réglementaires continueront d'évoluer et le cadre sera mis à jour en conséquence ; (4) l'usage principal est l'auto-évaluation organisationnelle et le suivi des progrès, et non la certification externe.

11.2 Hypothèses temporelles

Le modèle ne suppose pas de date précise pour les menaces quantiques ni pour l'achèvement de la migration. Les références au « futur » ou au « long terme » sont relatives. Les critères de contrôle qui font référence aux feuilles de route ou aux calendriers évaluent la présence d'une planification, et non l'adéquation des dates.

11.3 Hypothèses organisationnelles

Le modèle suppose une organisation (ou un périmètre défini) avec une gouvernance, des systèmes et des processus identifiables. Il ne suppose pas une taille, un secteur ou une structure particuliers ; l'applicabilité aux organisations très petites ou très distribuées peut nécessiter une interprétation de « l'organisation » et du périmètre des contrôles.

11.4 Limites connues

- Le PQMM ne se substitue pas à un audit cryptographique, un test d'intrusion ou une évaluation de conformité.
- Les résultats dépendent de l'exactitude et de l'exhaustivité de l'auto-déclaration organisationnelle.
- Le modèle ne vérifie pas l'exactitude des implémentations cryptographiques ni l'efficacité des contrôles.
- Le cadre ne certifie pas la conformité à une réglementation ou une norme.
- Les pondérations des dimensions sont fixes et peuvent ne pas refléter le profil de risque de chaque organisation.
- Les données de benchmark, lorsqu'utilisées, peuvent ne pas être représentatives.

11.5 Cas de non-applicabilité

Le cadre n'est pas conçu pour : (1) les environnements très classifiés ou de sécurité nationale sans adaptation ; (2) les contextes où la divulgation de la présence des contrôles est restreinte ; (3) un usage comme seule base pour la conformité contractuelle ou réglementaire ; (4) l'évaluation de produits ou fournisseurs individuels au-delà de leur rôle dans la préparation organisationnelle.

12. Gouvernance du modèle

12.1 Politique de versionnage

Le cadre est versionné (ex. 1.0). Les changements de version majeure peuvent introduire des changements structurels (dimensions, contrôles, agrégation) ; les changements de version mineure peuvent clarifier la rédaction ou ajouter des contrôles sans modifier l'agrégation. Les versions dépréciées sont documentées ; les utilisateurs sont encouragés à utiliser la version courante pour les nouvelles évaluations.

12.2 Déclencheurs de révision

Les révisions peuvent être déclenchées par : (1) des changements significatifs dans la normalisation (ex. nouvelles normes ou révisions NIST) ; (2) les retours utilisateurs et la revue méthodologique ; (3) l'évolution réglementaire ou de marché ; (4) une décision de gouvernance interne. Les changements sont documentés dans les notes de version.

12.3 Cycle de mise à jour

Il n'y a pas de calendrier fixe pour les mises à jour. Les mises à jour sont publiées lorsque les changements de méthodologie ou d'alignement justifient une nouvelle version. Les utilisateurs doivent vérifier la version courante lors de la comparaison de scores ou de la commande d'évaluations.

12.4 Possibilités de revue externe

L'éditeur peut solliciter une revue externe (académique, sectorielle ou organisme de normalisation) pour les versions majeures. Une telle revue ne constitue pas un aval formel. Tout processus de revue et ses résultats sont documentés de manière transparente.

12.5 Engagements de transparence

L'éditeur s'engage à : (1) documenter l'ensemble des contrôles, les pondérations et l'agrégation pour chaque version ; (2) énoncer clairement les hypothèses et les limites ; (3) publier l'historique des versions et les notes de version ; (4) ne pas laisser entendre une certification ou un aval là où il n'en existe pas.

13. Positionnement comparatif

13.1 Différences par rapport aux modèles de maturité cyber génériques

Les modèles de maturité cybersécurité génériques (ex. modèles larges basés sur le NIST CSF) couvrent un large éventail de contrôles. Le PQMM se concentre exclusivement sur la préparation post-quantique et la gouvernance, l'inventaire, l'infrastructure, la transition et la sensibilisation associées. Il ne remplace pas une évaluation de maturité générale ; il la complète par une vue spécifique PQC.

13.2 Complémentarité avec les cadres de risque d'entreprise

Le PQMM peut être utilisé aux côtés de la gestion des risques d'entreprise (ERM) et des cadres de risque opérationnel. Le risque PQC peut être enregistré dans les registres de risques et mappé aux dimensions du PQMM pour l'évaluation. Le cadre ne prescrit pas comment l'ERM intègre la PQC ; il fournit une manière structurée d'évaluer la préparation une fois le périmètre défini.

13.3 Énoncé de non-substitution

Le PQMM ne se substitue pas à : (1) un audit cryptographique ou de sécurité formel ; (2) des tests d'intrusion ou des exercices red team ; (3) une certification ISO 27001, SOC 2 ou similaire ; (4) une vérification de conformité légale ou réglementaire ; (5) une certification de fournisseur ou de produit. C'est un outil d'auto-évaluation et d'aide à la planification.

14. Guide de mise en œuvre

14.1 Préparation organisationnelle

Avant l'évaluation : définir le périmètre organisationnel (entité, division ou périmètre) ; s'assurer que les répondants ont accès aux politiques, inventaires et feuilles de route ; décider si le mode Rapide ou Complet est approprié pour l'usage prévu ; allouer du temps pour la collecte et la validation des données.

14.2 Engagement des parties prenantes internes

Impliquer la gouvernance (ex. RSSI, risque), les parties techniques (ex. infrastructure, développement) et conformité pour que les réponses reflètent l'état réel. Les évaluations à un seul répondant peuvent sous- ou sur-évaluer la maturité si une fonction n'a pas une visibilité complète.

14.3 Reporting à la direction générale

Présenter le QRI et le niveau comme un instantané de préparation ; utiliser les scores par dimension pour mettre en évidence les forces et les écarts ; éviter de prétendre à la « conformité » ou à la « sécurité » sur la seule base du modèle ; recommander une réévaluation périodique pour suivre les progrès.

14.4 Intégration à la gestion des risques d'entreprise

Mapper les dimensions du PQMM aux taxonomies de risque existantes ; enregistrer le risque PQC dans le registre de risques avec référence au niveau ou aux scores de dimensions du PQMM ; utiliser la feuille de route et les écarts de contrôles pour alimenter les plans de traitement du risque ; aligner le reporting sur les cycles ERM.

15. Conclusion

15.1 Implications stratégiques

La transition cryptographique post-quantique est un défi organisationnel pluriannuel. Un cadre de maturité structuré soutient la priorisation, l'allocation des ressources et la communication. Le PQMM fournit une base formelle et reproductible pour l'évaluation et le suivi, dans les limites d'un modèle d'auto-déclaration.

15.2 Perspective de gouvernance à long terme

La gouvernance du risque cryptographique restera pertinente à mesure que les standards et les menaces évoluent. Intégrer la préparation PQC dans la gouvernance de la politique, du risque et de l'architecture soutient la capacité de l'organisation à s'adapter à mesure que le NIST et les régulateurs publient de nouvelles orientations.

15.3 Impératif d'adaptation continue

Le cadre sera mis à jour à mesure que la normalisation et la réglementation évoluent. Les utilisateurs doivent considérer le PQMM comme une référence vivante et aligner leurs évaluations et feuilles de route sur la version courante et sur les évolutions externes.

16. Étapes pratiques d'adoption

Les organisations qui utilisent le PQMM progressent souvent selon une séquence de phases. Ce qui suit est une progression générique ; le calendrier et la profondeur dépendent du contexte et des moyens.

Sensibilisation et périmètre. Établir une compréhension partagée du risque post-quantique et du cadre. Définir le périmètre à évaluer (entité, division ou frontière de systèmes). Assigner la responsabilité et décider si le mode Rapide ou Complet est adapté pour la première évaluation.

Inventaire et gouvernance. Construire ou mettre à jour l'inventaire cryptographique et les artefacts de gouvernance (politiques, registre des risques, responsabilités). Réaliser une première évaluation PQMM pour obtenir un QRI et des scores par dimension de référence. Utiliser les résultats pour identifier les principaux écarts.

Priorisation et pilote. Prioriser les systèmes et actifs pour la migration (ex. par sensibilité, durée de vie et exposition). Planifier et réaliser un pilote limité (ex. une application ou un chemin d'échange de clés) pour valider l'interopérabilité et l'impact opérationnel. Affiner la feuille de route et les estimations de ressources.

Déploiement et suivi. Déployer la migration selon la feuille de route priorisée. Intégrer la préparation PQC dans la gouvernance continue (risque, conformité, architecture). Réexécuter l'évaluation PQMM périodiquement pour suivre les progrès et ajuster les plans.

Cette séquence est illustrative ; les organisations peuvent combiner ou réordonner les étapes selon leurs contraintes. Le PQMM accompagne chaque phase en fournissant une vue de maturité cohérente et une base pour le reporting et la priorisation.

Annexe A – Glossaire

Contrôle : Critère ou question discret utilisé pour évaluer un aspect d'une dimension. Chaque contrôle a un identifiant unique (ex. G01, C02) et est associé à une dimension, un tag (Direct, Migration, Hygiène) et une criticité (Critique, Élevé, Moyen, Faible).

Crypto-agilité : Capacité à remplacer ou ajouter des primitives cryptographiques (algorithmes, tailles de clé, protocoles) sans repenser les systèmes. En termes techniques : les systèmes exposent les choix cryptographiques via la configuration ou des modules interchangeables (ex. suites de chiffrement, accord de clés, algorithmes de signature) de sorte que le remplacement d'algorithme ne nécessite pas de changement de code ou d'architecture. La crypto-agilité est un prérequis pour une migration PQC progressive. Voir Annexe B.

Inventaire des actifs cryptographiques (CBOM) : Inventaire des actifs cryptographiques (certificats, clés, bibliothèques, protocoles) pouvant être affectés par la transition vers la cryptographie post-quantique.

Dimension : Un des cinq axes du PQMM : Gouvernance, Cryptographie, Infrastructure, Transition, Sensibilisation. Chaque dimension est évaluée via un ensemble de contrôles et contribue pour une part pondérée au QRI.

Harvest Now, Decrypt Later (HNDL) : Modèle de menace dans lequel un adversaire collecte des données ou communications chiffrées aujourd'hui et les conserve pour les déchiffrer lorsque une puissance de calcul suffisante (ex. un ordinateur quantique cryptographiquement pertinent) ou une avancée algorithmique devient disponible. Le HNDL implique que les données protégées uniquement par la cryptographie à clé publique classique peuvent être à risque futur ; il motive la priorisation des données à longue durée de vie et à haute sensibilité dans la migration PQC. Voir Annexe B.

Niveau de maturité : Un des cinq niveaux (0–4) dérivé de la bande de score QRI. Niveau 0 = Non conscient ; Niveau 1 = Sensibilisation initiale ; Niveau 2 = Évaluation structurée ; Niveau 3 = Transition maîtrisée ; Niveau 4 = Intégration stratégique.

Cryptographie post-quantique (PQC) : Algorithmes cryptographiques conçus pour résister aux attaques des ordinateurs classiques et quantiques. Dans ce document, la PQC désigne

en particulier les algorithmes standardisés par le NIST en 2024 : ML-KEM (encapsulation de clés, FIPS 203), ML-DSA (signatures module-réseau, FIPS 204) et SLH-DSA (signatures par hachage, FIPS 205), ou des normes internationales équivalentes. Voir Annexe B pour les catégories d'algorithmes PQC.

Préparation post-quantique : Dans ce cadre, la mesure dans laquelle une organisation a mis en place la gouvernance, l'inventaire, l'infrastructure, la planification de la transition et la sensibilisation nécessaires pour prendre des décisions éclairées sur l'adoption de la PQC et pour exécuter une migration maîtrisée. Voir Section 2.1.

Indice de préparation quantique (QRI) : Score numérique de 0 à 100, calculé comme la somme pondérée des cinq scores de dimensions. Le QRI détermine le niveau de maturité.

Mode rapide : Mode d'évaluation qui évalue un ensemble défini de contrôles essentiels (ex. 33) avec notation binaire uniquement. Utilisé pour la baseline et le suivi périodique.

Mode complet : Mode d'évaluation qui évalue l'ensemble complet des contrôles (ex. 92 contrôles) avec notation binaire et, le cas échéant, notation de la qualité du texte. Utilisé pour la planification détaillée de la migration et la préparation à la conformité.

Annexe B – Définitions formelles des concepts clés

Cryptographie post-quantique (PQC) : Mécanismes cryptographiques qui restent sûrs face aux attaques utilisant des ordinateurs quantiques à grande échelle. En pratique, le terme désigne les algorithmes standardisés par le NIST en 2024 (ML-KEM, ML-DSA, SLH-DSA dans FIPS 203, 204, 205) ou des normes internationales équivalentes. La PQC peut être déployée en mode hybride aux côtés des algorithmes classiques pendant la transition. **Catégories d'algorithmes PQC (NIST 2024) :** (1) **Encapsulation de clés :** ML-KEM (FIPS 203), à base de réseaux ; (2) **Signatures numériques — module-réseau :** ML-DSA (FIPS 204) ; (3) **Signatures numériques — par hachage :** SLH-DSA (FIPS 205). Ces catégories couvrent les principales fonctions (accord de clés, signatures) nécessaires à la migration ; le choix et la combinaison dépendent du cas d'usage et des mises à jour de normalisation.

Crypto-agilité : Propriété d'un système ou d'une organisation permettant de mettre à jour ou remplacer les primitives cryptographiques (algorithmes, longueurs de clé, protocoles) sans refonte ni redéploiement majeur. Techniquement cela implique : un choix centralisé ou paramétrable des algorithmes (ex. suites TLS, schémas de signature), une gestion des clés permettant la rotation d'algorithmes, et des chemins de mise à jour (ex. OTA, pilotés par configuration) le cas échéant. La crypto-agilité soutient la migration progressive vers la PQC et l'adaptation aux évolutions futures des standards.

Harvest Now, Decrypt Later (HNDL) : Modèle de menace dans lequel un attaquant capture des données ou communications chiffrées aujourd'hui et les conserve pour les déchiffrer lorsque une puissance de calcul suffisante (ex. un ordinateur quantique

cryptographiquement pertinent) ou une avancée algorithmique devient disponible. Le HNDL motive la priorisation des secrets à longue durée de vie ou à haute valeur pour la migration PQC. Les données à sensibilité temporelle ou à courte rétention peuvent être de priorité plus faible que les données à long horizon de confidentialité.

Schémas cryptographiques hybrides : Utilisation combinée d'un algorithme classique et d'un algorithme PQC pour la même fonction (ex. échange de clés ou signature) de sorte que la sécurité dépende des deux. Les schémas hybrides sont utilisés pendant la transition pour préserver la sécurité si un mécanisme est cassé.

Annexe C – Références normatives

Les normes et orientations suivantes sont référencées dans ce cadre. Les titres, éditions et années sont donnés pour citation ; les utilisateurs doivent confirmer les versions courantes lors de toute citation. La liste n'implique pas d'aval ou de certification de l'éditeur.

NIST Cryptographie post-quantique (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/CEI

- ISO/CEI 27001:2022, *Systèmes de management de la sécurité de l'information — Exigences* (dont le contrôle A.10 : Cryptographie).
- ISO/CEI 27002:2022, *Contrôles de sécurité — Contrôles pour la sécurité de l'information* (ex. Article 8.24 Contrôles cryptographiques, 8.25 Développement sécurisé).

Union européenne

- Directive (UE) 2022/2555 (NIS2) relative à des mesures pour un niveau élevé commun de cybersécurité.
- Règlement (UE) 2022/2554 (DORA) sur la résilience opérationnelle numérique du secteur financier.

Orientations nationales / agences

- ANSSI : *Avis de l'ANSSI sur la migration vers la cryptographie post-quantique* (2023–2024). Orientations de l'autorité nationale française sur la migration PQC.

https://cyber.gouv.fr

Autres

- Publications ENISA sur la cryptographie post-quantique.
- ETSI Quantum-Safe Cryptography : https://www.etsi.org/technologies/quantum-safe-cryptography

Annexe D – Modèle de visualisation radar

Un graphique radar (araignée) peut être utilisé pour afficher les cinq scores de dimensions sur un même graphique. Chaque axe représente une dimension (Gouvernance, Cryptographie, Infrastructure, Transition, Sensibilisation). Le score de chaque dimension (0–100) est reporté sur l'axe correspondant ; les points sont reliés pour former un polygone. Cela permet une comparaison visuelle de l'équilibre entre dimensions. La même échelle (0–100) doit être utilisée pour tous les axes. Le QRI global n'est pas représenté directement sur le radar ; c'est la somme pondérée des cinq valeurs de dimensions.

Visuels méthodologiques. Le flux d'évaluation peut être résumé ainsi : *Contrôles (par dimension) → score de dimension (0–100) → agrégation pondérée → QRI (0–100) → niveau de maturité (0–4).* Un schéma de ce flux, et un exemple de graphique radar avec les scores par dimension, sont disponibles dans la démo interactive Qubixor à l'adresse https://qubixor.com/demo (vues rapport et benchmark). Ils illustrent la forme du livrable sans prescrire un outil spécifique.

Annexe E – Modèle de rapport dirigeant

Structure suggérée pour un résumé exécutif d'une page des résultats PQMM :

1. **Périmètre :** Organisation ou périmètre évalué ; date d'évaluation ; version du cadre et mode (Rapide/Complet).
2. **Résultat global :** Score QRI (0–100) ; niveau de maturité (0–4) avec libellé court.
3. **Synthèse par dimension :** Tableau ou radar avec les cinq scores de dimensions ; mettre en évidence la ou les dimensions les plus faibles.
4. **Écarts clés :** Jusqu'à trois écarts prioritaires dérivés des résultats au niveau des contrôles (aucune inférence au-delà de ce que le modèle évalue).
5. **Prochaines étapes :** Actions recommandées (ex. construire l'inventaire, formaliser la feuille de route, assigner la responsabilité).
6. **Réserves :** L'évaluation est basée sur l'auto-déclaration ; elle ne constitue pas un audit ni une attestation de conformité.

Exemple de livrable. Un exemple concret du format de rapport PQMM—score QRI, radar des dimensions, synthèse et actions prioritaires—est disponible dans la démo interactive Qubixor à l'adresse https://qubixor.com/demo. La démo montre comment le livrable du cadre est présenté en pratique (rapport de maturité, comparaison benchmark, vue écosystème) sans imposer un outil ou fournisseur particulier.
