PASC

PAN-AFRICAN STANDARDS COUNCIL

DIRECTIVE / INSTITUTIONAL EDITION

PASC-Q01 · ED. 1.0 · NOVEMBER 2026

Quantum cryptographic transition and assurance

Cryptographic inventory · Transition · Quantum assurance

Issuing authority
Pan-African Standards Council (PASC)

Publication status
Council-approved · Published

Publication date
1 November 2026

Official standards library
pasc.institute

Defined requirements
Auditable evidence
Controlled editions

Institutional architecture

PASC OSPCRM Q01 extends OSPCRM v1.0 with additional decisions, technical evidence and transition controls for exposure from quantum-vulnerable cryptography. OSPCRM supplies contextual prioritisation, sovereignty analysis, performance evidence, operational integration and demonstrable certification. The existing P0–P4 classification, FNR protocol, certification architecture and AI/supplier clauses continue to govern their respective domains.

1 Scope

1.1 This directive specifies requirements for identifying, assessing, migrating, operating and validating cryptographic dependencies whose security may be affected by advances in quantum computation.

1.2 It applies to organizations and products or services adopting the quantum domain profile, including public administration, essential services, financial systems, healthcare, education, research, cloud, identity systems, IoT/OT, connected products, supplier-managed systems and archival services.

1.3 Cryptographic uses within scope include confidentiality, key establishment, digital signatures, identity assertions, PKI, device and software signing, code and firmware integrity, authentication, backup, inter-service communication and long-lived records. The assessment SHALL include provider-controlled cryptography and critical supplier dependencies.

1.4 The directive governs transition and assurance, not the design or approval of novel cryptographic algorithms. Research constructions do not qualify as approved production mechanisms solely by satisfying this management directive.

2 Normative status and terminology

2.1 OSPCRM v1.0 remains the governing standard for risk methodology, organizational context, control-plane sovereignty, metrics, operations and conformance. A certified quantum profile SHALL additionally satisfy this directive within its declared scope.

2.2 **SHALL** denotes a requirement; **SHOULD** a recommendation; **MAY** permission. Exceptions to SHALL requirements are nonconformities unless an explicit exception mechanism is stated in that clause. A risk-acceptance record is not proof that a failed mandatory technical control passed.

2.3 A *cryptographic dependency* is a use of cryptography by an asset, protocol, product, trust service, data flow or supplier on which a protected objective depends. A *cryptographic bill of materials* (CBOM) is a versioned inventory of such dependencies, including the evidence supporting discovery and coverage.

2.4 *Quantum-vulnerable cryptography* means an algorithm or protocol whose intended security properties are materially threatened by a relevant quantum attack under the organization’s declared threat model. *PQC* means post-quantum cryptography. *Crypto-agility* means an evidenced capability to replace or update cryptographic mechanisms with acceptable continuity and security.

2.5 A *harvest-now-decrypt-later* exposure occurs where an adversary may retain protected communications or data today and exploit future cryptanalytic capabilities during the information's required secrecy lifetime.

2.6 A *hybrid establishment* combines classical and post-quantum methods through a specified and assessed mechanism. Merely invoking two algorithms is not sufficient evidence of secure composition.

3 Governance and accountability

Q.GV.01 The OSPCRM Risk Model Owner SHALL approve a quantum transition policy identifying protected missions, confidentiality and signature-validity horizons, acceptable mechanisms, responsible owners and escalation authorities.

Q.GV.02 Each in-scope critical service SHALL have an accountable service owner, cryptography owner and supplier owner where applicable. Owners SHALL identify dependencies outside their administrative control, including PKI, KMS, HSMs, hardware firmware, cloud control planes and certificate authorities.

Q.GV.03 The organization SHALL maintain a versioned quantum migration roadmap with priority, approved design, implementation status, independent acceptance result, dependencies, contingency and decision authority. The roadmap SHALL be reviewed after material cryptographic standards changes, compromises, platform changes or significant new evidence.

Q.GV.04 The policy SHALL distinguish binding laws and contracts from voluntary guidance and transition roadmaps in each applicable jurisdiction. No global deadline SHALL be inferred solely from another jurisdiction's recommendation.

4 Discovery and cryptographic inventory

Q.IN.01 The organization SHALL maintain a CBOM linked to its OSPCRM asset, service, dependency, data-classification and supplier inventories. The CBOM SHALL cover cryptography in transit, at rest, signing, authentication, attestation and recoverability where relevant.

Q.IN.02 Each material record SHALL include, where applicable: asset and service identifier; accountable owner; cryptographic purpose; protocol and protocol version; implementation or library; algorithm and parameter set; key lifecycle and storage; certificate or trust chain; data class; service dependency; vendor or control-plane jurisdiction; migration and update mechanism; operational constraints; source and date of evidence; and inventory confidence.

Q.IN.03 Unidentified cryptographic mechanisms and inaccessible supplier components SHALL be recorded as unresolved dependencies, not omitted from coverage percentages. Critical and P0/P1 services SHALL have a documented method for detecting hidden dependencies through protocol inspection, software analysis, provider attestations or tested sampling.

Q.IN.04 Automated discovery SHALL be reconciled with architecture records, procurement records, software and firmware inventories, key-management evidence and service-owner attestations. A simple algorithm count SHALL NOT constitute a complete inventory claim.

5 Quantum exposure and OSPCRM prioritisation

Q.RA.01 Quantum transition priorities SHALL use the existing OSPCRM P0–P4 methodology, including asset and service consequence, exposure, threat, temporal factors, control effectiveness and sovereignty. The directive introduces no competing priority scale.

Q.RA.02 For each material cryptographic dependency, the assessment SHALL consider: information secrecy lifetime; future signature or trust-verification lifetime; feasibility of collecting protected material today; migration lead time; feasibility of replacing dependent products; ability to revoke or reissue trust; potential safety or service consequences; provider concentration; and confidence in the threat assumption.

Q.RA.03 Where protected information may remain valuable beyond the credible cryptographic protection period, the organization SHALL explicitly evaluate harvest-now-decrypt-later exposure. It SHALL use scenario ranges and documented assumptions rather than assert a precise date for the arrival of a cryptographically relevant quantum computer.

Q.RA.04 The assessment SHALL include irreversible or expensive-to-reverse consequences: historical disclosure, persistent forgery, compromised firmware trust, invalid archive signatures, identity trust-chain failure and supplier lockout. Long-lived records MAY require earlier treatment than short-lived traffic on otherwise similar systems.

Q.RA.05 Each P0/P1 quantum exposure SHALL have a dated owner decision, containment or migration plan, service-level objective aligned with OSPCRM, and independently testable closure conditions. Documented risk acceptance SHALL retain the original exposure and residual-risk record.

6 Cryptographic transition controls

Q.TR.01 The organization SHALL specify an approved cryptographic profile for each relevant use case, with exact algorithms, parameter sets, implementation constraints, protocol variants, validation expectations and supplier requirements.

Q.TR.02 For applicable public-key use cases, approved profiles SHOULD draw on finalized NIST FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA) and application-specific standards and approved protocols. Key-encapsulation uses SHALL follow applicable composition, key-derivation and usage recommendations, including NIST SP 800-227 where adopted. Profiles SHALL be updated as relevant recognized standards evolve.

Q.TR.03 The organization SHALL distinguish key establishment, digital signing, data encryption, hashing and authentication. It SHALL NOT misclassify ML-KEM as a standalone bulk-data cipher or assume all symmetric cryptography is automatically quantum-broken.

Q.TR.04 Hybrid deployment MAY be used where it is supported by an approved specification and tested implementation. It SHALL have explicit failure handling, anti-downgrade behaviour, algorithm negotiation rules, key separation or combiner assurance as relevant, and evidence that both peers actually negotiate the intended protection.

Q.TR.05 The migration plan SHALL cover protocol and certificate interoperability, device constraints, message size, handshake and signing performance, hardware-backed keys, backup and restoration, long-lived signatures, root-of-trust replacement and supplier update cadence.

Q.TR.06 The organization SHALL protect signing and decapsulation keys, establish authorized key-rotation and revocation processes, and test recovery from key compromise and failed upgrade. Migration SHALL not silently relax existing confidentiality, integrity or authentication controls.

Q.TR.07 Critical systems SHALL support a tested contingency for transition failure. Rollback SHALL not constitute permanent permission to retain deprecated protection, and it SHALL not silently re-enable a weaker negotiated mode.

7 Testing and demonstrable assurance

Q.AS.01 Transition acceptance SHALL require representative testing of key establishment or signing, protocol interoperability, configuration enforcement, downgrade resistance, failure modes, performance, resilience and operational recovery. Manufacturer statements alone SHALL not count as completed testing.

Q.AS.02 Tests SHALL include negative cases: absent PQC support, incorrect parameter sets, expired or revoked credentials, corrupted signatures, failed encapsulation or decapsulation, certificate-chain incompatibility, fallback attempts and misconfigured peers.

Q.AS.03 Critical implementations SHALL include verification against known-answer or approved implementation tests and risk-appropriate side-channel, fault-injection and secret-handling analysis. Test scope and findings SHALL remain auditable.

Q.AS.04 The organization SHALL establish an independent acceptance authority proportionate to consequence. For P0/P1 exposures the verifier SHALL not rely solely on the migration implementer’s declaration.

Q.AS.05 An exposure may be marked *controlled* only when the specified cryptographic path, dependent services and required trust properties have passed the acceptance criteria. Ticket closure, software-version change or supplier marketing status alone SHALL not establish closure.

8 Metrics and reporting

Q.ME.01 Quantum-profile reporting SHALL preserve OSPCRM FNR, P0/P1 precision and other applicable core metrics. It SHALL additionally include:

- Critical cryptographic dependency discovery coverage with explicit unknowns;
- Fraction of P0/P1 quantum exposures with a current owner and approved treatment;
- Fraction of P0/P1 exposures independently verified as controlled;
- Time between risk determination, implementation and acceptance;
- Unsupported or untested downgrade/fallback paths;

- Supplier migration commitments and missed milestones;
- Failed migration or recovery tests, with corrective status.

Q.ME.02 Metrics SHALL state the population, denominator, observation window, evidence source and scope. Unsupported claims of total quantum safety SHALL not appear in PASC conformity reports.

9 Conformance profiles

Q.CO.01 An organization claiming OSPCRM Quantum Profile Conformance SHALL meet the applicable OSPCRM baseline and every SHALL requirement in this directive within a documented service and cryptographic scope.

Q.CO.02 A product or service claim SHALL identify supported use cases, algorithms, protocols, validated configurations, exclusions, dependencies and acceptance-test results. A general “quantum ready” assertion does not establish conformance.

Q.CO.03 PASC certification SHALL follow the existing PASC evidence and assessor rules. The certificate record SHALL show the OSPCRM base version, directive version, scope, review date, tested configurations, material exceptions, expiry and verification reference. Certification SHALL be withheld where evidence fails the declared control objective.

Q.CO.04 Material changes to cryptographic implementations, critical trust dependencies, supported algorithms, control-plane operators or accepted risk SHALL trigger change review and, where warranted, targeted reassessment.

Annex A — Minimum evidence set (Normative)

The quantum-profile evidence package SHALL contain: (A1) approved policy and risk ownership; (A2) CBOM with completeness method and unknowns; (A3) service/data secrecy-lifetime analysis; (A4) OSPCRM decision records; (A5) migration and supplier roadmap; (A6) configuration and cryptographic profiles; (A7) test plan and positive/negative results; (A8) key and certificate lifecycle records; (A9) contingency and recovery test; (A10) independent acceptance report; (A11) metrics and corrective action ledger.

Annex B — Representative acceptance scenarios (Informative)

B1 Long-term confidential records: demonstrate a crypto inventory, interception exposure analysis, approved migration path, successful authorized communication and negative downgrade test. The finding remains open if a dependent archival export uses the old protection.

B2 Signatures on long-lived government records: demonstrate trust-chain and evidence-preservation continuity, replacement of vulnerable signing mechanisms, and independent verification of records after certificate rollover.

B3 Constrained industrial device: demonstrate supported implementation, operational impact, fallback behaviour and recovery after a failed firmware or trust-anchor update. Safety and continuity remain part of the OSPCRM consequence assessment.

Annex C — Relationship to OSPCRM and external references (Informative)

Directive topic	Existing OSPCRM v1.0 clauses retained	Added quantum-specific requirement
Governance	5 and 6	Q.GV cryptographic transition ownership and policy
Inventory and context	7	Q.IN cryptographic bill of materials and unknown coverage
Priority	6, 7 and 9	Q.RA temporal quantum exposure without a second risk score
Sovereignty and suppliers	8.4 and 8.5	Crypto trust and vendor transition dependencies
Operations and metrics	9 and 10	Q.TR, Q.AS and Q.ME migration testing and acceptance
Conformance	11	Q.CO profile-scoped technical evidence

References

1. PASC, *Open Sovereign Predictive Cyber Risk Management*, v1.0, November 2025, https://doi.org/10.5281/zenodo.17642943.
2. NIST, FIPS 203, *Module-Lattice-Based Key-Encapsulation Mechanism Standard*, August 2024, https://doi.org/10.6028/NIST.FIPS.203.
3. NIST, FIPS 204, *Module-Lattice-Based Digital Signature Standard*, August 2024, https://doi.org/10.6028/NIST.FIPS.204.
4. NIST, FIPS 205, *Stateless Hash-Based Digital Signature Standard*, August 2024, https://doi.org/10.6028/NIST.FIPS.205.
5. NIST, SP 800-227, *Recommendations for Key-Encapsulation Mechanisms*, September 2025, https://doi.org/10.6028/NIST.SP.800-227.
6. NIST, IR 8547, *Transition to Post-Quantum Cryptography Standards*, final edition, 27 October 2026, https://csrc.nist.gov/pubs/ir/8547/final (informative transition resource).
7. European Commission and Member States, *Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*, June 2025, https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography (informative roadmap, not universal law).

Annex D — French administrative summary (Informative)

Intitulé : Directive spéciale PASC OSPCRM Q01 relative à la transition cryptographique post-quantique et à sa vérification. **Objet :** compléter OSPCRM v1.0 par des obligations techniques relatives à l’inventaire cryptographique, à la durée de confidentialité, aux risques de collecte actuelle et de déchiffrement futur, à la migration, à l’agilité cryptographique et à la démonstration indépendante des résultats. L’échelle P0–P4, la souveraineté opérationnelle et les exigences de certification d’OSPCRM demeurent applicables.