MARCH 2026
APPLIED QUANTUM

THE APPLIED QUANTUM PQC MIGRATION FRAMEWORK

TELECOMMUNICATIONS EXTENSION

Mobile Operators, Fixed-Line Carriers, and Converged Network Providers — *Industry-Specific Challenges and Framework Adaptations*

Version 1.1 — March 2026

Marin Ivezic
CEO, Applied Quantum
Author, PostQuantum.com

PQCFramework.com | PostQuantum.com | SecureQuantum.com | AppliedQuantum.com

"Start while it's a project, before it's a crisis."

COPYRIGHT AND LICENSE

DISCLAIMER

This extension is provided as professional guidance based on the author's and Applied Quantum's practitioner experience and publicly available standards, regulations, and industry research. It does not constitute legal, regulatory, financial, or compliance advice. Organizations should consult qualified legal counsel, auditors, and regulatory authorities for guidance specific to their jurisdiction, sector, and circumstances.

The regulatory timelines, vendor capabilities, algorithm parameters, and tool categories referenced in this document reflect the state of the PQC landscape as of March 2026. This landscape evolves rapidly. Readers should verify current status against primary sources Readers should verify current status against primary sources (NIST, NSA, ETSI, 3GPP, GSMA, national agencies, vendor documentation) before making implementation decisions.

References to specific vendors, products, or tools are for illustrative purposes and do not constitute endorsement.

NIST IR 8547, referenced throughout for deprecation and disallowance timelines, was an Initial Public Draft as of November 2024 with final publication expected in 2025–2026. Federal agencies and their contractors should reference the final published version when available.

ABOUT THIS DOCUMENT

Document type	Enterprise methodology and practitioner framework
Parent Document	The Applied Quantum PQC Migration Framework — Universal — v1.1 (March 2026)

Intended audience	CISOs, security architects, network engineers, compliance officers, and program managers in telecommunications operators and infrastructure providers
Assumed knowledge	Familiarity with the Universal PQC Migration Framework and its 8-phase lifecycle; working knowledge of mobile/fixed network architectures, 3GPP standards, and telecom security
Scope	Industry-specific challenges and phase-by-phase framework adaptations for telecommunications. Not a standalone document — intended to be used alongside the Universal Framework.

HOW TO USE THIS EXTENSION

This document is a companion to the Applied Quantum PQC Migration Framework (Universal). It does not replace the Universal Framework but extends it with telecommunications-specific guidance. For each topic, this extension identifies unique sector challenges and then maps specific adaptations to the relevant Universal Framework phase. Readers should have the Universal Framework open alongside this document and cross-reference its phase definitions, maturity indicators, and templates.

ACCOMPANYING RESOURCES

Every aspect of this framework — from executive business cases and cryptographic inventory methodologies to CBOM architecture, hybrid deployment patterns, and vendor governance — has been analyzed in detail on PostQuantum.com over the past 10+ years through practitioner-grounded articles, deep dives, and sector-specific analyses.

The best starting point is the curated Quantum Readiness Starting page: https://postquantum.com/quantum-readiness-starting/ — but readers should also use PostQuantum.com's Search function to surface additional relevant posts that may not be included in that curated list.

Key framework resources, templates, and supporting materials are also published on PQCFramework.com — a dedicated companion site for this framework, drawing on relevant content from PostQuantum.com.

TABLE OF CONTENTS

WHY TELECOMMUNICATIONS REQUIRES A SECTOR EXTENSION

The Universal PQC Migration Framework provides a comprehensive 8-phase methodology applicable to any enterprise. Telecommunications operators can and should follow that methodology. However, the telecommunications sector faces a distinct combination of constraints that make PQC migration more complex, more technically intricate, and more vendor-dependent than in most other industries. These constraints do not invalidate the Universal Framework — they sharpen, extend, and occasionally reorder its guidance.

This section identifies the characteristics that set telecommunications apart.

Critical National Infrastructure with Unmatched Cryptographic Breadth

Telecommunications networks are arguably the most critical infrastructure in any modern economy — every other sector depends on them. They are also among the most cryptography-dense environments in existence. A single 5G voice call with roaming traverses subscriber authentication (5G-AKA), SUPI concealment (ECIES), radio-layer encryption (SNOW 3G, AES, ZUC), core network TLS/IPsec across dozens of network functions, inter-operator security gateways (SEPP), IMS signaling security, and backend billing/CDR integrity. Each of these uses distinct cryptographic algorithms, keys, and trust anchors managed by different entities.

This breadth means that cryptographic inventory (Phase 1) and CBOM documentation (Phase 2) are orders of magnitude more complex in telecommunications than in a typical enterprise. A real-world CBOM exercise for a single Open RAN deployment covers hundreds of distinct cryptographic instances across the O-RU, O-DU, O-CU, RIC, SMO, and virtualization layers — and that is only the radio access network.

Extreme Vendor Dependency

Most enterprises control the majority of their own cryptographic estate. Telecommunications operators do not. The network — from base stations and transport routers to SIM cards, IMS platforms, and OSS/BSS — is overwhelmingly vendor-supplied, and much of it is proprietary. An operator cannot unilaterally switch a base station's IPsec module to PQC algorithms; it must wait for the vendor to release firmware or hardware that supports them. The same is true for SIM/UICC secure elements, session border controllers, GGSN/PGW gateways, and virtually every network element.

This vendor dependency is the binding constraint on migration timelines. Unlike financial services, where the primary coordination challenge is multi-party transaction flows, telecommunications' primary constraint is that the operator does not own the code running on most of its infrastructure. The Universal Framework's Phase 7 (Vendor & Supply Chain) must be elevated to an active, ongoing workstream from Phase 0 onward — not treated as a late-stage activity.

The 3GPP Standards Bottleneck

Telecommunications is among the most standards-governed industries in the world. Cryptographic choices in mobile networks are not at the operator's discretion — they are specified by 3GPP in excruciating detail. An operator cannot deploy PQC-protected 5G-AKA or quantum-safe SUPI concealment until 3GPP defines the algorithms, key sizes, and protocol modifications in a formal Release. As of March 2026, 3GPP has study items underway for PQC integration in 5G-Advanced and 6G, but finalized specifications are not expected before Release 19 or 20.

This creates a fundamental tension: operators face regulatory and threat-driven urgency to migrate, but cannot change most network-layer cryptography until standards bodies act. The framework must account for this by identifying which cryptographic layers operators can migrate independently (transport IPsec/TLS, management plane, OSS/BSS) and which require standards-body progress (AKA, SUPI concealment, RAN ciphering).

Massive Physical Footprint and Long Equipment Lifecycles

A large mobile operator may have 50,000–200,000 cell sites, each containing radio units, baseband processors, power systems, and backhaul equipment with embedded cryptographic functions. Fixed-line carriers add millions of customer-premises devices

(CPE), optical transport nodes, and access network elements. This equipment is designed for 10–20 year lifecycles — far longer than typical IT refresh cycles.

Many of these devices run on constrained processors with limited memory, making PQC adoption challenging even when vendor firmware is available. The larger ML-KEM public keys and ML-DSA signatures impose real computational and bandwidth costs on embedded systems. Phase 6 (Infrastructure & Performance) must include a hardware capability assessment that is far more granular than what most enterprises require.

Lawful Interception and National Security Obligations

Telecommunications operators are legally required to provide lawful interception (LI) capabilities in virtually every jurisdiction. LI systems depend on the ability to intercept, decrypt, and reconstruct communications at specific network points. PQC migration must not break LI functionality — a constraint that does not apply to most other industries.

This has implications for how hybrid cryptography is deployed, where key escrow or key disclosure mechanisms operate, and how regulators are engaged during migration planning. In some jurisdictions, regulators must approve changes to LI architecture before they are deployed. This regulatory dependency adds timeline risk that must be explicitly modeled in Phase 4 (Roadmap & Governance).

Inter-Operator Coordination and Roaming

A mobile call or data session frequently traverses multiple operator networks. International roaming requires bilateral security agreements, interconnect gateways (SEPPs in 5G), and shared trust anchors between home and visited networks. Migrating these interfaces to PQC requires coordinated action between operators who may be on different continents, subject to different regulations, and using equipment from different vendors.

The GSMA plays a coordination role analogous to card networks in financial services, but with far less centralized control. Unlike a card network that can mandate a specific algorithm by a certain date, the GSMA issues guidelines that operators adopt voluntarily. This makes roaming interfaces among the hardest elements to migrate — and among the most exposed to HNDL interception on international transit links.

Convergence of IT, OT, and Network Technology

Modern telecom operators run a complex mix of traditional network elements (which behave more like OT — long-lived, vendor-controlled, safety/uptime-critical), cloud-

native network functions (which behave like IT), and massive OSS/BSS platforms. PQC migration must span all three domains simultaneously, each with different change management processes, risk tolerances, and vendor landscapes. The Universal Framework's distinction between IT and OT environments applies, but telecom adds a third category — network infrastructure — that shares characteristics of both.

INDUSTRY-SPECIFIC CHALLENGES

This section details the technical and operational challenges unique to telecommunications PQC migration. Each challenge is presented with its technical basis, real-world evidence, and the Universal Framework phases it most directly impacts. Section 3 then maps these challenges to specific framework adaptations.

Challenge 1: 5G-AKA and SUPI Concealment Quantum Vulnerability

The 5G authentication framework relies on 5G-AKA (or EAP-AKA'), which is symmetric-key based and therefore not directly vulnerable to Shor's algorithm. However, SUPI concealment — the mechanism that protects subscriber identity over the air interface — uses ECIES (Elliptic Curve Integrated Encryption Scheme) with the home network's public key. A quantum computer running Shor's algorithm would break ECIES, re-exposing subscriber identities and effectively reverting 5G's privacy protections to 4G-era vulnerability. This is not a theoretical risk: SUPI encryption keys are provisioned in SIM cards, meaning that remediation requires both a 3GPP specification update and a SIM replacement or remote reprovisioning campaign affecting every subscriber.

> **Framework Impact:** Phase 1 (Discovery) must map all ECIES usage in SUPI concealment. Phase 5 (Pilots) must include SIM/eSIM reprovisioning pilots. Phase 7 (Vendor) must track SIM vendor PQC readiness.

Challenge 2: Radio Access Network Constrained Environments

Radio units (O-RUs in Open RAN, or proprietary RRHs) and baseband units operate on embedded processors with strict latency, power, and memory constraints. These devices handle RAN-layer ciphering (SNOW 3G, AES-128, ZUC) and IPsec tunnels on fronthaul/midhaul interfaces. While the symmetric ciphers used for air-interface encryption are not directly quantum-vulnerable, the IPsec key exchange on fronthaul (ECIES, DH, ECDH) is. Upgrading IPsec on tens of thousands of cell-site devices to support ML-KEM hybrid handshakes introduces larger packets, higher computational overhead, and potential compatibility issues with middleboxes and transport optimizers.

The challenge is compounded by the physical footprint: cell-site visits for hardware upgrades are expensive (estimated at $500–1,500 per site), and many operators have equipment from multiple vendors at each site. Firmware updates that change cryptographic behavior require extensive regression testing to avoid service disruption.

> **Framework Impact:** Phase 1 must include RAN hardware capability assessment (processor, memory, firmware version). Phase 6 must model handshake-size impacts on fronthaul bandwidth. Phase 4 must sequence RAN upgrades across the cell-site estate.

Challenge 3: Core Network Service-Based Architecture Complexity

5G core networks use a service-based architecture (SBA) where dozens of network functions (AMF, SMF, UPF, NRF, UDM, AUSF, etc.) communicate over HTTP/2 with mutual TLS. Each inter-NF connection uses TLS 1.2 or 1.3 with ECDHE key exchange and X.509 certificates. Migrating this mesh to PQC-protected TLS requires updating every network function's TLS stack, reissuing certificates with PQC algorithms, and ensuring that the Network Repository Function (NRF) and SCP (Service Communication Proxy) can handle larger PQC handshakes and certificate chains.

The number of TLS connections in a 5G core is enormous — in a large operator, the NF mesh may involve hundreds of distinct service endpoints, each maintaining multiple persistent TLS sessions. Performance testing must verify that PQC-TLS handshakes do not degrade control-plane latency beyond acceptable thresholds for call setup, mobility management, and session establishment.

> **Framework Impact:** Phase 2 (CBOM) must document every NF-to-NF TLS configuration. Phase 5 must include SBA-wide PQC-TLS pilot. Phase 6 must benchmark control-plane latency with PQC handshakes under realistic load.

Challenge 4: Inter-Operator Security and Roaming Interfaces

The 5G Security Edge Protection Proxy (SEPP) mediates all signaling between operators for roaming. SEPPs use TLS and additionally apply JSON Object Signing and Encryption (JOSE) to protect HTTP messages at the application layer. Both the TLS transport and the JOSE signatures/encryption use quantum-vulnerable asymmetric algorithms. Migrating SEPP-to-SEPP connections to PQC requires bilateral agreement between operators, aligned vendor support, and potentially coordinated certificate infrastructure changes.

The legacy SS7/Diameter signaling interconnect (still widely used for 2G/3G/4G roaming) presents an even harder problem: these protocols have minimal cryptographic protection

to begin with, and upgrading them is constrained by decades-old equipment and the complexity of global roaming agreements. The IPX (IP Packet Exchange) providers that carry inter-operator traffic add another coordination layer.

> **Framework Impact:** Phase 3 (Risk Scoring) must weight roaming interfaces for HNDL exposure on international transit. Phase 4 must model bilateral operator coordination timelines. Phase 7 must include GSMA engagement for coordinated roaming PQC migration.

Challenge 5: Lawful Interception Architecture Dependencies

Lawful interception (LI) systems are architecturally embedded in the network and depend on specific cryptographic access points. LI compliance in most jurisdictions requires that the operator can deliver intercepted content in a decryptable form to law enforcement agencies. PQC migration must not disrupt this capability.

Changes to key exchange mechanisms, session key derivation, or encryption modes may require corresponding updates to LI mediation devices and delivery interfaces. In some cases, regulators must review and approve changes to LI architecture before network-wide deployment. This creates a hidden regulatory dependency that can delay PQC rollout if not identified and managed early.

> **Framework Impact:** Phase 0 must include LI regulatory engagement. Phase 4 must incorporate LI compliance checkpoints. Phase 5 must verify LI functionality in PQC pilot environments.

Challenge 6: SIM/eSIM and Device Ecosystem Constraints

The SIM (UICC/eSIM) is the hardware root of trust for mobile subscriber authentication. Current SIMs store ECIES public keys for SUPI concealment and execute the AKA algorithm using symmetric keys. Deploying PQC-protected SUPI concealment requires SIMs that support PQC key encapsulation — meaning new SIM hardware or secure element firmware from SIM vendors (Thales, IDEMIA, G+D, etc.).

The installed base of SIMs globally is measured in billions. Even for a single operator with 50–100 million subscribers, replacing or reprovisioning SIMs is a multi-year logistics and customer-experience challenge. eSIM (eUICC) technology offers remote provisioning capability, but PQC support in eSIM profiles depends on the eSIM platform vendor and the GSMA's RSP (Remote SIM Provisioning) specification, which has not yet incorporated PQC.

On the device side, handset operating systems (Android, iOS) must support PQC in their TLS stacks for data connections. Apple and Google have begun integrating PQC into their platforms (Apple's iMessage PQ3, Chrome's ML-KEM support), but enterprise MDM and VPN configurations add additional complexity.

> **Framework Impact:** Phase 1 must inventory SIM types and eSIM platform versions. Phase 4 must plan SIM migration campaigns. Phase 7 must track SIM vendor and device OEM PQC roadmaps.

Challenge 7: Transport and Backhaul Network Scale

Telecom transport networks (DWDM optical, MPLS/IP, microwave backhaul, satellite) carry all traffic between cell sites, aggregation points, and data centers. These networks use IPsec, MACsec, and OTN-layer encryption with key exchange mechanisms that are quantum-vulnerable. The transport network may involve equipment from multiple vendors (Ciena, Nokia, Huawei, Cisco, Ericsson) with different upgrade paths and PQC timelines.

PQC key exchange increases handshake sizes, which can fragment packets and interact poorly with MTU constraints on some transport links. Microwave backhaul with limited bandwidth is particularly sensitive to PQC overhead. Satellite backhaul (common in rural and maritime deployments) combines bandwidth constraints with high latency, making PQC handshake round-trips more costly.

> **Framework Impact:** Phase 1 must inventory transport encryption endpoints. Phase 6 must benchmark PQC handshake overhead on bandwidth-constrained links. Phase 7 must coordinate across transport equipment vendors.

Challenge 8: OSS/BSS and IT System Sprawl

Telecom operators typically run hundreds of OSS/BSS applications for network management, provisioning, billing, CRM, and service assurance. These systems use TLS for inter-system communication, X.509 certificates for authentication, and database encryption for subscriber data at rest. Many are legacy applications from vendors who may no longer actively support them.

Unlike the network layer (which is governed by 3GPP), OSS/BSS systems are under the operator's control and can be migrated independently. This makes them attractive early-migration targets — but the sheer number of systems, interfaces, and certificate dependencies creates a coordination challenge that rivals the network itself.

> **Framework Impact:** Phase 1 should prioritize OSS/BSS systems as independently migratable. Phase 4 should sequence OSS/BSS migration as a quick-win track parallel to network-layer work.

Challenge 9: IoT/M2M and Private Network Exposure

Telecom operators are significant providers of IoT connectivity (NB-IoT, LTE-M, 5G mMTC) and increasingly offer private 5G networks for enterprise customers. IoT devices are typically the most constrained endpoints in the network — low power, minimal processing, deployed for 10–15 year lifecycles. Many cannot be firmware-updated and some use cryptographic implementations that will never support PQC.

Private 5G networks add complexity because the operator may share responsibility for security with the enterprise customer. The boundary of the operator's PQC migration scope becomes blurred, and contractual frameworks for shared quantum readiness are essentially nonexistent.

> **Framework Impact:** Phase 1 must inventory IoT/M2M device populations and capabilities. Phase 3 must score IoT segments for HNDL risk. Phase 7 must address private network customer coordination.

Challenge 10: Open RAN Multi-Vendor Cryptographic Fragmentation

Open RAN architecture disaggregates the radio access network into components from different vendors (O-RU, O-DU, O-CU, RIC, SMO), each potentially using different cryptographic libraries, certificate infrastructure, and key management approaches. Unlike traditional single-vendor RAN deployments where one vendor controls the entire cryptographic estate, Open RAN distributes cryptographic responsibility across multiple suppliers.

This fragmentation complicates CBOM documentation, increases the number of vendor coordination threads for PQC migration, and introduces interoperability risk when different vendors adopt PQC at different rates. The O-RAN Alliance's security specifications must also evolve to support PQC, adding another standards-body dependency alongside 3GPP.

> **Framework Impact:** Phase 2 must produce per-component CBOMs across the Open RAN stack. Phase 5 must include multi-vendor PQC interoperability testing. Phase 7 must coordinate across O-RAN Alliance members.

PHASE-BY-PHASE FRAMEWORK ADAPTATIONS FOR TELECOMMUNICATIONS

This section walks through each Universal Framework phase and specifies the adaptations, additions, and re-prioritizations required for telecommunications. Organizations should implement these alongside — not instead of — the Universal Framework's phase guidance.

Phase 0 — Executive Mandate & Business Case

Additional Business Case Arguments

- **Critical infrastructure designation:** Telecommunications operators are designated critical infrastructure in virtually every jurisdiction. Quantum vulnerability in telecom infrastructure is a national security concern, not merely a corporate risk. Frame the business case in terms of national security obligations and the operator's role as infrastructure provider to every other sector.
- **Regulatory convergence:** Map the convergence of NIST/CNSA 2.0 timelines, EU NIS2 Directive requirements for critical infrastructure, national telecom regulator expectations, and GSMA post-quantum guidelines. The argument is not "regulators require PQC today" but "the regulatory trajectory makes PQC investment inevitable — early movers face lower costs and less disruption."
- **HNDL exposure on interconnect:** International transit links (submarine cables, IXPs, IPX networks) are high-value HNDL targets. Quantify the volume of signaling and subscriber data traversing these links daily. This produces a concrete "data-at-risk" metric for board reporting.
- **Competitive differentiation:** As enterprise customers (especially government, defense, and financial services) begin requiring quantum-safe connectivity from their carriers, early PQC readiness becomes a sales advantage. SK Telecom's and Deutsche Telekom's public quantum security initiatives demonstrate this positioning.

Governance Adaptation

Establish a Quantum Readiness Steering Committee that includes representation from Network Engineering, IT/BSS, Security, Regulatory Affairs, and Procurement. The network engineering function must have co-equal status with security — in telecom, PQC migration is as much a network transformation as a security program. Include regulatory affairs from day one to manage LI compliance, spectrum allocation implications, and national security reporting requirements.

Phase 1 — Discovery & Inventory

Expanded Scope: Telecom-Specific Inventory Tracks

The Universal Framework's discovery methodology must be extended with parallel inventory tracks specific to telecommunications:

- **RAN inventory track:** Cell-site equipment catalog (vendor, model, firmware version, cryptographic capabilities). For Open RAN, separate inventories per disaggregated component (O-RU, O-DU, O-CU). Include hardware crypto acceleration capabilities (e.g., AES-NI, no PQC equivalent yet).
- **Core network inventory track:** 5G SBA network function catalog with per-NF TLS configuration, certificate issuer, and key exchange algorithm. Map the NF communication mesh — which NF talks to which, and what TLS profile is used for each connection.
- **Transport inventory track:** Encryption endpoints on DWDM, MPLS, microwave, and satellite links. Identify which transport segments use MACsec vs. IPsec vs. OTN encryption and the key exchange mechanisms for each.
- **Interconnect inventory track:** SEPP configurations for roaming partners. SS7/Diameter security proxy configurations. IPX provider security capabilities.
- **SIM/device inventory track:** SIM types deployed (2FF, 3FF, 4FF, eSIM), SUPI concealment support, ECIES key profiles. Device population by OS version and PQC capability.
- **OSS/BSS inventory track:** Application catalog with TLS configurations, certificate dependencies, database encryption methods, and vendor support status.

Risk-Driven Scoping for Telecommunications

Given the scale (a large operator may have 500,000+ distinct systems and interfaces), full cryptographic inventory is a multi-year effort. Apply the Universal Framework's risk-driven scoping methodology, but with telecom-specific prioritization: begin with international interconnect (highest HNDL exposure), then core network SBA mesh (highest TNFL risk to subscriber data integrity), then transport encryption, then RAN, then OSS/BSS, then IoT/M2M.

Phase 2 — CBOM & Documentation

Telecommunications CBOM Complexity

A telecommunications CBOM is inherently more complex than a typical enterprise CBOM because cryptographic usage spans multiple protocol layers (radio, transport, signaling, application) and multiple trust domains (operator, vendor, partner operator, standards body). Apply the Universal Framework's Minimum Viable CBOM approach aggressively: document the architecture-layer CBOM first (which protocol on which interface uses which algorithm class), then fill in implementation-level detail incrementally.

The Open RAN CBOM exercise described on PostQuantum.com demonstrates the level of detail required for a single RAN subsystem. Scale this across core, transport, OSS/BSS, and interconnect to estimate the full CBOM scope.

3GPP Protocol Alignment

Map CBOM entries to 3GPP specification references (e.g., TS 33.501 for 5G security, TS 33.210 for network domain security). This alignment is essential because it identifies which cryptographic instances the operator can change unilaterally and which require 3GPP specification changes. Tag each CBOM entry with its standards dependency status: "operator-controlled," "vendor-dependent," or "standards-dependent."

Phase 3 — Risk Scoring & Prioritization

Adapted Risk Scoring Model

The Universal Framework's risk scoring model uses five dimensions: data sensitivity, cryptographic vulnerability, exposure to interception, migration difficulty, and regulatory/compliance urgency. For telecommunications, add two additional dimensions:

- **Standards dependency:** Does migrating this system require 3GPP or O-RAN Alliance specification changes? Systems that are standards-dependent score higher on migration difficulty because the operator cannot control the timeline.
- **Multi-operator coordination:** Does migrating this system require bilateral or multilateral coordination with other operators? Roaming interfaces and interconnect gateways score highest because migration cannot be completed unilaterally.

Telecommunications Priority Tiers

Priority	System Category	Rationale
Tier 1	International interconnect (SEPP, IPX), management plane TLS/SSH, OSS/BSS with subscriber data	Highest HNDL exposure, operator-controlled, can migrate without standards-body dependency. Immediate risk reduction.
Tier 2	Core network SBA mesh (inter-NF TLS), transport encryption (IPsec/MACsec), PKI/certificate infrastructure	High exposure, largely vendor-dependent but not standards-dependent. Migration possible with vendor firmware updates.
Tier 3	5G-AKA/SUPI concealment, RAN-layer interfaces, SIM ecosystem	Critical but standards-dependent. Plan now, execute when 3GPP specifications and vendor implementations are available.
Tier 4	IoT/M2M device populations, legacy 2G/3G infrastructure, satellite backhaul	Hardware-constrained or low-urgency. Apply compensating controls (segmentation, overlay encryption) while planning long-term replacement.

Phase 4 — Roadmap & Governance

External Dependency Mapping

Telecommunications roadmaps must explicitly model three categories of external dependency that most enterprises do not face:

- **Standards-body timelines:** 3GPP Release schedules for PQC-enabled specifications. O-RAN Alliance security specification updates. GSMA post-quantum guideline evolution.
- **Vendor delivery timelines:** Per-vendor PQC firmware/software release dates for each major equipment category (RAN, core, transport, SIM). Track these as external milestones in the program plan.

- **Inter-operator coordination timelines:** Bilateral roaming agreement updates. GSMA-coordinated migration windows for interconnect protocols.

Recommended Year-1 Plan Adaptations

In addition to the Universal Framework's year-1 plan, telecom operators should:

- **Q1:** Launch 3GPP and GSMA engagement tracks. Issue PQC readiness RFIs to top-5 network equipment vendors. Begin LI regulatory pre-engagement.
- **Q2:** Complete Tier 1 (interconnect and management plane) cryptographic inventory. Begin OSS/BSS TLS migration pilots.
- **Q3:** Complete core network SBA CBOM. Begin transport encryption vendor coordination. Initiate SIM vendor PQC roadmap discussions.
- **Q4:** Deliver first board report with data-at-risk metrics for interconnect HNDL exposure. Publish internal PQC migration policy. Begin Tier 2 pilot planning.

Phase 5 — Pilots & Migration Execution

Telecommunications Pilot Targets

Telecom pilots must address the unique multi-layer, multi-vendor nature of the network. Recommended pilot sequence:

- **Pilot 1 — Management plane:** Migrate SSH and TLS on network management interfaces (NMS, EMS, orchestration platforms) to hybrid PQC. Low risk, high learning value, operator-controlled.
- **Pilot 2 — OSS/BSS inter-system TLS:** Select 2–3 internal BSS application interfaces and deploy hybrid ML-KEM-768 + X25519 TLS. Measure latency and compatibility.
- **Pilot 3 — Transport IPsec:** Deploy hybrid PQC IPsec on a non-production transport segment (e.g., lab or disaster-recovery link). Test MTU behavior, fragmentation, and middlebox compatibility.
- **Pilot 4 — Core network NF mesh:** In a lab/staging 5G core, migrate inter-NF TLS to PQC. Benchmark control-plane call-setup latency under load.
- **Pilot 5 — SEPP/roaming (coordinated):** Bilateral pilot with a willing roaming partner to test PQC-protected SEPP-to-SEPP signaling. Requires GSMA coordination.

The Hybrid Architecture Reality

Telecom networks will operate in hybrid mode (classical + PQC) for an extended period — likely 5–10 years or longer. Unlike an enterprise that might complete a full TLS migration in 2–3 years, a telecom operator must manage coexistence across protocol layers (some PQC-ready, some not), vendor ecosystems (some upgraded, some lagging),

and inter-operator boundaries (some partners migrated, some not). Crypto-agility is not optional in telecom — it is the only viable architecture.

Phase 6 — Infrastructure Modernization & Performance

Network Impact Assessment

PQC introduces measurable performance impacts that must be tested across the telecom-specific infrastructure:

- **Handshake overhead on SBA mesh:** ML-KEM-768 adds approximately 1,100 bytes to TLS ClientHello. In a dense SBA mesh with thousands of connections, test aggregate impact on control-plane throughput and session-establishment latency.
- **Certificate chain bloat:** ML-DSA-65 certificates are approximately 20x larger than ECDSA certificates. Test impact on OCSP/CRL checking overhead, especially for short-lived NF certificates.
- **Fronthaul bandwidth:** Test PQC IPsec overhead on bandwidth-constrained eCPRI fronthaul links. Determine whether PQC handshake sizes require MTU adjustments or fragmentation handling.
- **Microwave and satellite backhaul:** Model PQC handshake round-trip costs on high-latency satellite links and bandwidth-limited microwave hops.

HSM and Key Management Modernization

Telecom operators rely on HSMs for SIM personalization, certificate issuance, and lawful intercept key management. These HSMs must support PQC algorithms. Engage HSM vendors (Thales Luna, Entrust nShield, Utimaco) early to understand their PQC roadmaps and certification timelines (FIPS 140-3, Common Criteria).

Phase 7 — Vendor & Supply Chain Governance

Telecommunications Vendor Classification

Classify vendors by their impact on PQC migration timeline:

- **Tier A — Timeline-blocking:** RAN vendors (Ericsson, Nokia, Samsung, Huawei), SIM vendors (Thales, IDEMIA, G+D), core network vendors. These vendors' PQC readiness directly determines when the operator can migrate specific network layers. Engage at CTO-to-CTO level.
- **Tier B — Timeline-influencing:** Transport equipment vendors, OSS/BSS platform vendors, HSM vendors. These can be migrated on the operator's schedule but

require vendor firmware/software support. Standard vendor management engagement.

- **Tier C — Operator-controlled:** In-house developed applications, internal tools, custom integrations. Migrate on the operator's timeline using internal engineering resources.

Industry Coordination Forums

Telecom operators must actively participate in industry forums that influence PQC standardization and coordination:

- **3GPP SA3 (Security):** The working group defining PQC integration in mobile network specifications. Participation is essential to influence timeline and algorithm choices.
- **GSMA Post-Quantum Taskforce:** Coordinates operator-to-operator migration planning, roaming interface PQC guidelines, and SIM ecosystem PQC requirements.
- **O-RAN Alliance Security Focus Group:** Defines security specifications for Open RAN, including PQC requirements for disaggregated RAN components.
- **ETSI TC CYBER QSC:** Develops quantum-safe cryptography standards applicable to European telecom operators.
- **National telecom regulators:** Pre-engage on LI implications, critical infrastructure PQC mandates, and compliance timelines.

TELECOMMUNICATIONS REGULATORY ALIGNMENT MAP

This table maps key regulatory and standards drivers to their PQC migration implications for telecommunications operators.

Authority / Standard	Requirement	Timeline	Telecom Implication
NIST / CNSA 2.0	Deprecate classical asymmetric algorithms; adopt ML-KEM, ML-DSA	2030 deprecation, 2035 disallowance	Affects all TLS/IPsec in operator infrastructure. Mandatory for operators serving US government customers.
EU NIS2 Directive	Critical infrastructure must implement state-of-the-art security measures	Transposition by Oct 2024; enforcement ongoing	Telecom operators are essential entities under NIS2. PQC readiness is increasingly expected as state-of-the-art.
3GPP (SA3)	PQC integration in 5G-Advanced / 6G security specifications	Study items in Rel-19; normative specs expected Rel-20 (2027–2028)	Defines when operators can deploy standards-compliant PQC for AKA, SUPI, and SBA security.
GSMA PQ Guidelines	Post-Quantum Cryptography Guidelines for Telecom Use Cases (PQ.03)	Published 2024; updates expected	Non-binding but industry-coordinating. Defines algorithm preferences and roaming migration guidance.

ETSI QSC	Quantum-safe cryptography technical specifications	Multiple TRs published; ongoing	Applicable to European operators. Aligns with EU Cyber Resilience Act requirements.
National CI regulators	Critical infrastructure quantum readiness mandates (varies by jurisdiction)	France ANSSI: 2030 target; others emerging	Direct compliance obligations for operators designated as critical infrastructure. LI implications require early engagement.
O-RAN Alliance	Security specifications for disaggregated RAN	Ongoing updates	Defines PQC requirements for multi-vendor RAN. Affects Open RAN adopters specifically.

TELECOM MATURITY MODEL SUPPLEMENT

The Universal Framework's 5-level maturity model applies to telecommunications with the following sector-specific indicators:

Level	Universal Indicator	Telecom-Specific Indicator
Level 1: Aware	Executive sponsorship secured; quantum risk acknowledged	CISO/CTO joint sponsorship. 3GPP SA3 participation initiated. LI regulatory pre-engagement begun.
Level 2: Assessed	Cryptographic inventory complete for priority systems; CBOM initiated	Tier 1 (interconnect, management plane) inventory complete. Core SBA CBOM initiated. SIM inventory by type/vendor. RAN hardware capability baseline.
Level 3: Planning	Risk-scored migration roadmap approved; pilots designed	Multi-track roadmap (operator-controlled, vendor-dependent, standards-dependent) approved. SIM vendor and RAN vendor PQC timelines integrated. LI compliance plan reviewed by regulators.
Level 4: Migrating	Hybrid PQC deployed in production for priority systems; CBOM maintained	Tier 1 systems migrated to hybrid PQC. Core SBA TLS migration underway. Transport encryption PQC rollout in progress. GSMA roaming PQC coordination active.
Level 5: Resilient	Crypto-agile architecture operational; all quantum-vulnerable crypto remediated or compensated	Full network PQC coverage (or compensating controls for standards-dependent layers). Crypto-agile architecture embedded in NF lifecycle. CBOM maintained across all domains. Roaming interfaces PQC-protected.

TELECOMMUNICATIONS KPI SUPPLEMENT

Board-Level KPIs (Quarterly)

- **Interconnect HNDL exposure:** Percentage of international interconnect traffic (SEPP, IPX, transit) protected by PQC or hybrid cryptography.
- **Network-layer PQC coverage:** Percentage of TLS/IPsec connections across the SBA mesh, transport, and management plane using PQC or hybrid key exchange.
- **Vendor PQC readiness:** Percentage of Tier A vendors with confirmed PQC-capable firmware/software delivery dates within 18 months.
- **Standards-body alignment:** Active participation status in 3GPP SA3, GSMA PQ Taskforce, and relevant national regulator consultations.
- **Regulatory compliance trajectory:** Gap analysis score against NIS2, CNSA 2.0, and applicable national CI mandates.

Operational KPIs (Monthly)

- **Cryptographic inventory coverage:** Percentage of network domains (RAN, core, transport, OSS/BSS, interconnect) with completed cryptographic inventory.
- **CBOM freshness:** Percentage of CBOM entries verified within the last 90 days.
- **PQC pilot progress:** Number of pilot phases completed / planned. Latency and compatibility results from active pilots.
- **SIM migration readiness:** Percentage of subscriber base on PQC-capable SIM/eSIM profiles (once available).
- **Transport PQC rollout:** Number of transport encryption endpoints migrated to hybrid PQC / total endpoints.

RECOMMENDED IMMEDIATE ACTIONS

For telecommunications operators that have not yet begun PQC migration planning, the following actions can be taken immediately — regardless of where 3GPP or vendor timelines stand:

- **1. Secure executive mandate with joint CISO/CTO sponsorship.** Frame quantum readiness as both a national security obligation and a network modernization opportunity. Use interconnect HNDL exposure as the urgency metric.
- **2. Begin Tier 1 cryptographic inventory immediately.** Focus on management plane (SSH, TLS on NMS/EMS), international interconnect (SEPP, IPX), and OSS/BSS with subscriber data. These are operator-controlled and can be inventoried and migrated without waiting for 3GPP or vendors.
- **3. Issue PQC readiness RFIs to your top network equipment vendors.** Ask specifically: what is your timeline for PQC-capable firmware for [specific product lines]? What algorithms will you support? Will hybrid mode be available? Document responses and integrate into program planning.
- **4. Engage 3GPP SA3 and GSMA PQ Taskforce.** If not already participating, join these working groups. PQC specification decisions being made now will determine your migration options for the next decade.
- **5. Pre-engage your national telecom regulator on LI implications.** Do not wait for regulators to ask about PQC. Proactively brief them on your migration plans and solicit guidance on LI compliance requirements for PQC-protected network elements.
- **6. Launch a management-plane PQC pilot.** Deploy hybrid ML-KEM + X25519 TLS on a subset of network management interfaces. This builds internal competency, validates tooling, and generates data for the broader migration plan — all without touching subscriber-facing services.
- **7. Inventory your SIM estate and initiate SIM vendor discussions.** Understand what SIM types are deployed, what eSIM penetration exists, and what your SIM vendors' PQC roadmaps look like. SIM migration will be the longest-lead-time activity for SUPI concealment protection.

FURTHER READING

The following PostQuantum.com articles provide deep-dive analysis on topics covered in this extension:

- **Telecom Quantum Readiness: Why the Urgency and Where to Start** — https://postquantum.com/post-quantum/telecom-quantum-readiness-start/
- **Quantum-Readiness / PQC Full Program Description (Telecom Example)** — https://postquantum.com/post-quantum/quantum-readiness-telco/
- **Telecom's Quantum-Safe Imperative: Challenges in Adopting PQC** — https://postquantum.com/post-quantum/telecom-pqc-challenges/
- **Cryptographic Bill of Materials (CBOM) for an Open RAN-Based Telecom RAN** — https://postquantum.com/post-quantum/cbom-open-ran-telecom/
- **Cryptography in a Modern 5G Call: A Step-by-Step Breakdown** — https://postquantum.com/post-quantum/cryptography-telecommunications-5g/
- **Quantum Readiness and Multi-Party Cryptographic Coordination (MCC)** — https://postquantum.com/post-quantum/quantum-mcc/
- **Hybrid Cryptography for the Post-Quantum Era** — https://postquantum.com/post-quantum/hybrid-cryptography-pqc/
- **Introduction to Crypto-Agility** — https://postquantum.com/post-quantum/introduction-crypto-agility/
- **Infrastructure Challenges of "Dropping In" Post-Quantum Cryptography** — https://postquantum.com/post-quantum/infrastructure-challenges-pqc/
- **PQC and Network Connectivity: Challenges and Impacts** — https://postquantum.com/post-quantum/pqc-network-impacts/
- **Upgrading OT Systems to PQC: Challenges and Strategies** — https://postquantum.com/post-quantum/ot-pqc-challenges/

ABOUT

ABOUT THE AUTHOR

Marin Ivezic is a former Fortune Global 500 CISO/CTO, the Editor-in-Chief of PostQuantum.com, and the founder and CEO of Applied Quantum. He previously held cybersecurity partner and practice lead roles — including regional and global leadership positions — at IBM, Accenture, PwC, and KPMG. He is also the former CEO of Cyber Agency and the founder of Cryptosec, a cryptography advisory and engineering firm.

Marin has been involved in quantum technologies for over 25 years, having advised governments on the quantum threat since the early 2000s. He previously founded Boston Photonics and PQ Defense. He has led real-world quantum readiness programs for telecoms, financial institutions, and critical infrastructure operators — including programs exceeding 120,000 discrete migration tasks.

PostQuantum.com, his personal blog, reaches over 1 million monthly readers and is recognized as the premier quantum security publication for CISOs, CTOs, and security architects worldwide.

ABOUT APPLIED QUANTUM

Applied Quantum (AppliedQuantum.com) is a research-driven professional services firm focused entirely on quantum technologies and post-quantum security. Its dedicated security practice, Secure Quantum (SecureQuantum.com), focuses on quantum security advisory and PQC migration. Services span Quantum Security & PQC Migration, Quantum Strategy & Sovereignty, Quantum Engineering & Implementation, and Quantum Commercialization.

If you need help: Applied Quantum provides advisory, program design, and hands-on migration execution support. Contact: contact@appliedquantum.com