SEPTEMBER 2026

APPLIED QUANTUM

THE APPLIED QUANTUM PQC MIGRATION FRAMEWORK

TELECOMMUNICATIONS EXTENSION

Mobile networks, fixed-line and interconnect *– sector-specific challenges and framework adaptations*

Version 3.0 – September 2026

Marin Ivezic

CEO, Applied Quantum

Author, PostQuantum.com

Disclosure: Applied Quantum provides post-quantum migration advisory services. This work is published openly under CC BY 4.0 and is usable without engaging Applied Quantum.

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

COPYRIGHT AND LICENSE

DISCLAIMER

This framework 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 PQC as of September 2026. These references may become outdated quickly. Readers should verify current status against primary sources before making implementation decisions; movement between editions is published through the PQC Migration Brief.

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, remains an Initial Public Draft at the date of this edition; the deprecation and disallowance dates it proposes are cited as anchors and re-checked at each release. Federal agencies and their contractors should reference the final version when it publishes.

ABOUT THIS DOCUMENT

Document type	Enterprise methodology and practitioner framework
Parent document	The Applied Quantum PQC Migration Framework – Universal – v3.0 (September 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 v3.0 and its 8-phase lifecycle; working knowledge of mobile and fixed network architectures, 3GPP specifications and release planning, GSMA coordination, and telecom security
Scope	Industry-specific challenges and phase-by-phase framework adaptations for telecommunications: mobile and fixed operators,

	interconnect and roaming, transport, the SIM and device ecosystems, and the OSS/BSS estate. Not a standalone document – intended to be used alongside the Universal Framework.
Status	Version 3.0 - published September 2026

VERSION HISTORY

Version	Date	Changes
2.0	June 2026	Major version. Three methodological changes: (1) two-track migration model separating key exchange (HNDL) and signature/PKI (TNFL) as parallel tracks; (2) PKI architecture fork with definitive position on Merkle Tree Certificates for public Web PKI; (3) FIPS 140-3 validation gap as hard deployment constraint with environment classification. New Program Foundation sections: SOC Implementation (five detection use cases, four incident response playbooks, five tabletop exercises, three-horizon quantum CTI model), GRC Implementation (17-indicator cascading KRI framework, risk appetite statements, regulatory intelligence process, audit and assurance, GRC-SOC handoff). Expanded Program Foundations: Governance (program leadership, board oversight, three lines of defense), Crypto-Agility (five-dimensional operational discipline with four-year implementation roadmap), Skills & Team Structure (team sizing, build/borrow/buy framework, crypto champion program). Also added: cost estimation methodology, NIST CSWP 39 crypto-agility alignment, 2026–2030 regulatory deadline convergence analysis, multinational hybrid navigation framework, deployment ecosystem status data, algorithm pipeline update (9 additional signature candidates, FN-DSA/HQC status, CNSA 2.0 requirements), objection-handling appendix (Appendix F). All sector extensions updated to v2.0.
2.1	June 2026	Targeted update. Activity 3.3 sequencing harmonized with the two-track model; explicit position on hybrid/composite signatures; algorithm-specific vulnerability weighting added to Phase 3 risk scoring (ECC/RSA quantum resource analysis); SP 800-208 hash-based signatures foregrounded as the deploy-now component of Track B. New: Activity 2.5 (Secure the CBOM and Program Artifacts), Migration Verification & Program Closure section, identity and authentication stack in Track B scope. Added: reference program economics (0.2c), confidentiality-horizon method (1.1), evidence dossier as

Version	Date	Changes
		litigation defense, M&A due diligence, procurement model-language references, additional common failures and benefit arguments. Web PQC adoption datapoint corrected to F5 Labs mid-2025 attribution. Companion book (Quantum Ready) cross-references added. Also added: data-at-rest decision framework (5.6); AI-assisted migration position (5.7) with a Phase 1 tool category; counterparty coordination (7.6); cloud shared responsibility and SaaS (7.7); Accelerated Execution Profile (4.7); risk-weighted coverage KPI; algorithm sovereignty and standards fragmentation; crisis communications and industry information sharing (GRC); skills matrix; role-based reading paths and right-sizing profiles; Appendix G (framework crosswalk); Appendix H (protocol coverage matrix).
3.0	September 2026	Major version, published with Universal v3.0. Crypto-agility as the program's method read for operator estates: the agility objective stated for the sector (an operator is crypto-agile when it can change the algorithm on the layers it controls on a planned date and can name the graded date on which each standards-bound or peer-bound interface follows its standard or its peer), the agility criterion and a rehearsal per wave on the management plane, the SBA policy, the SEPP and the NF issuing CA, "migrated with agility debt" as the recorded state for shared interfaces the peer cannot change and for the standards-bound layers, and closure at zero unaccepted agility debt read against the roaming and interconnect population. Alignment section rebuilt on v3.0: validation decided per product (CMVP #5247) with operators serving government inheriting FIPS-required slices as written; three new subsections (the agility criterion and rehearsal; evidence grades and the coverage denominator; vendor dates and questions). Phase adaptations mirror the v3.0 method: dual-outcome charter, named owners and the three lines by function (Phase 0); evidence grades and the enumerated denominator on the six inventory tracks (Phase 1); the minimum record with the Profile as informative carriage and prefixed CBOM layers (Phase 2); the four dimensions by name, the two telecom additions restated as factors inside Dimension 3 with the arithmetic, verifier updatability per entry and a delivery-state column in the priority tiers (Phase 3); firmness grades on every external date, two results per gate record and the Re-Baseline Protocol (Phase 4); pilots at standards currency

Version	Date	Changes
		(X25519MLKEM768 per RFC 9954 and RFC 10024 on the SBA and N32; RFC 10042 SSH on the management plane; hybrid IKEv2 per RFC 9370 on transport), resumption by mode, dated retirement of pre-standard code points and the rehearsal per wave (Phase 5); the four-field HSM and KMS register with entropy references and the transport-by-protocol reading (Phase 6); questionnaire order, certificate-authority questions, the one-afternoon test and the CCF cross-reference on vendor concentration (Phase 7). Standards currency: 3GPP TR 33.703, the Release 20 256-bit algorithm sets and the Release 21 timeline agreed June 2026; the GSMA PQ series PQ.01 to PQ.07 dated from the GSMA document page, with PQ.05 (roaming, July 2025) and PQ.06 (hybrid key-exchange prototype verification, May 2026) added. Regulatory map rebuilt at four columns with status and enforcement-tier columns and the jurisdiction roster replaced by the Global PQC Migration Clock pointer; the E1 currency sentence on national telecom regulators. Corrections made in the open: the "PQ.03 v2.0" suffix removed (the series is PQ.01 to PQ.07, PQ.03 dated October 2024); the five-dimension scoring residue replaced by the Universal's four; the CNSA 2.0 row that carried NIST IR 8547's dates removed for the pointer. Selectable vendor names moved to Tool and Vendor References; the three network equipment providers kept as a public fact. Maturity supplement on the Universal's 0 to 5 scale; four agility KPIs with the interconnect HNDL exposure KPI kept as the urgency metric; two immediate actions added. Requirements register generated as Appendix J. About block aligned to the Universal.

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: mobile and fixed network operators, interconnect and roaming, transport, the SIM and device ecosystems, and the OSS/BSS estate. 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.

WHAT'S NEW IN V3.0

Version 3.0 of the Telecommunications Extension publishes with Universal Framework v3.0 (September 2026). Crypto-agility is the program's organizing method and measured end state, and

this extension states the ruling for operators: an operator is crypto-agile when it can change the algorithm on the layers it controls (the management plane, OSS/BSS, the SBA TLS policy, the SEPP configuration, its own PKI, the transport concentrators) on a planned date and can name the graded date on which each standards-bound or peer-bound interface follows its standard or its peer, so the agility criterion and the rehearsal per wave run on those layers, "migrated with agility debt" is the recorded state for the shared interfaces a peer cannot change and for the layers 3GPP and the SIM still own, and closure requires zero unaccepted agility debt read against the roaming and interconnect population. Regulatory content states the mechanism and the sector's own bodies with status and enforcement tier; national telecom regulators now issue transition-plan requirements, and a regulator that sets a date is a row on the Global PQC Migration Clock page, where the jurisdiction roster is maintained beside the Universal's Regulatory Timeline Context.

What moved since June 2026, and what did not. 3GPP agreed the Release 21 timeline at its June 2026 plenaries (package approval and Stage-1 freeze March 2027; Stage-2 freeze June 2028; Stage-3 freeze December 2028; ASN.1 and OpenAPI freeze March 2029), and SA3's Release 20 study on the transition to post-quantum cryptography (TR 33.703, independent of any generation) is published and under change control since June 17, 2026, with version 20.0.0 approved at SA#112 and uploaded June 25, 2026 and version 20.0.1 uploaded July 3, 2026 under work item FS_CryptoPQC (UID 1080045); it completed on its Release 20 schedule, the normative work packages follow from it, and a published technical report is not a deployable profile. The June 2026 edition of this extension, and a verification pass earlier in this release that read 3GPP's narrative page rather than the specification record, both described the study as in progress and past its target date; the specification record is the primary source and the status is corrected here. Release 20 introduces the 256-bit algorithm sets for 5G (TS 35.240 to TS 35.248). The GSMA Post-Quantum Telco Network Task Force's series now runs PQ.01 to PQ.07 as listed on its document page, and this edition adds PQ.05 (Quantum-safe Cryptography for 4G and 5G Roaming, July 2025) and PQ.06 (Implementation and Prototype Verification of Post-Quantum Use Case: Hybrid Key Exchange, May 2026) as the references for the SEPP and roaming pilot; PQ.07 (non-terrestrial networks) is dated February 2026 as published. The hybrid TLS groups moved onto the standards track (RFC 9954 and RFC 10024, with X25519MLKEM768 Recommended=Y and the Kyber768 draft code points obsoleted) and hybrid SSH published as RFC 10042; the pilots, the SBA and N32 text and the management-plane action are restated on them, the IPsec transport text is matched to the Universal's Appendix H row (hybrid IKEv2, RFC 9370), and every long-lived NF, SEPP and management session is covered by the Universal's resumption-by-mode rule. Nothing else sector-specific moved: no national telecom regulator instrument is verified and named in this edition, the O-RAN Alliance status is carried from June 2026 unchecked, and the GSMA Remote SIM Provisioning specifications are carried at their June 2026 state with a re-verification instruction.

Alignment section and adaptations. Three technical statements are stated exactly at this edition: where the SUCI is computed (3GPP TS 31.102 provides both mobile-equipment and USIM calculation, selected per subscription by EF_UST services 124 and 125, so the card campaign covers the USIM-calculation population and not every subscriber; Challenges 1 and 6, Phase 1); the two protection modes of N32 (TLS, or PRINS with symmetric JWE on N32-f keyed from the N32-c handshake, so the asymmetric dependency sits in the N32-c and TLS-mode N32-f handshakes, the certificates and the intermediaries' JWS signatures; Challenge 4, Phase 1, Pilot 5); and the symmetric 5G-AKA and RAN ciphering populations, whose 3GPP question is the 256-bit algorithm sets and not a Shor exposure. The alignment section is rebuilt on v3.0: the validation subsection states the per-product rule (CMVP certificate #5247, April 2026) and keeps, as written, that operators serving government customers inherit FIPS-required slices; the verification subsection is rewritten to the four verification

dispositions and closure at zero unaccepted debt, read against roaming and interconnect peers, with the closure proof run on the SEPP, the management plane and the NF issuing CA; and three subsections are added: the agility criterion and rehearsal in telecommunications; evidence grades and the coverage denominator in telecommunications; vendor dates and questions in telecommunications. The phase adaptations mirror the v3.0 method where this extension already adapts the element: the dual-outcome charter, the Crypto-Agility and Cryptographic Record owners in network engineering and the three lines by function (Phase 0); evidence grades and the enumerated denominator on the six inventory tracks (Phase 1); the minimum record with the Applied Quantum CBOM Profile as informative carriage and the CBOM layers prefixed (Phase 2); the four dimensions by name, the telecom additions restated as factors inside Dimension 3 with the Universal's arithmetic, verifier updatability read per entry, the priority tiers re-derived from the Universal's ordered test (SUCI concealment, the burned-in anchors and the radio-path transport segments in Tier 1, each blocked entry with its bridging pattern recorded), and a delivery-state column where "dependent" is the common state for the standards-bound layers (Phase 3); firmness grades on every standards, vendor and peer date, two results per gate record and the Re-Baseline Protocol (Phase 4); the rehearsal per wave and the wave-exit criterion (Phase 5); the four-field HSM and KMS register with entropy references, with the SIM personalization, NF issuing CA and lawful-interception modules as standing rows (Phase 6); and the questionnaire order, the certificate-authority questions for the NF PKI, vendor CAs and the eSIM issuers, the one-afternoon test against proprietary quantum-safe claims, and the Cryptographic Concentration Framework cross-reference on vendor concentration, with no figure computed here (Phase 7).

Supplements, corrections and currency. The maturity supplement is re-based on the Universal's 0 to 5 scale with the Universal's level names, and the KPI supplement gains the four agility KPIs measured on the layers the operator changes, with the interconnect HNDL exposure KPI kept as the sector's urgency metric and a classical-only acceptance line for the dual stack on roaming. Two immediate actions are added: name a Crypto-Agility owner in network engineering, and schedule the first rehearsal on the management-plane pilot. Three statements of the June 2026 edition are corrected in the open: it cited a version suffix on GSMA PQ.03 that the GSMA's document list does not carry (the series is PQ.01 to PQ.07, PQ.03 dated October 2024); its Phase 3 text scored risk on a five-dimension list that the Universal had already replaced with four; and its regulatory map carried NIST IR 8547's 2030 and 2035 dates in a CNSA 2.0 row, which is replaced by the pointer to the Universal's roster. Selectable vendor names (SIM vendors, transport equipment vendors, HSM products, a fourth RAN vendor) move from the body to Tool and Vendor References; the three network equipment providers the Universal names as a concentration fact stay in the body, and the operators the June 2026 edition cited as positioning examples are not carried. Further Reading adds the July 2026 HNDL analysis, the Global PQC Migration Clock and the two NIS2 analyses. Appendix J lists the extension's own requirements.

WHAT'S NEW IN V2.1

Version 2.1 of the Telecommunications Extension is a major alignment release tracking Universal Framework v2.1 (June 2026). Because the extension moves directly from v1.1, it adopts the Universal v2.0 structural foundations and the v2.1 positions in a single release:

Alignment with Universal Framework v2.1. A new alignment section maps the two-track migration model, the FIPS validation gap in carrier infrastructure, and the Merkle Tree Certificates position onto operator estates, followed by six v2.1 position subsections: hybrid and composite signatures in network infrastructure; algorithm weighting and the ECC-heavy 5G core; subscriber and network

identity in Track B; SP 800-208 for network element and eSIM firmware; CBOM protection and the network map problem; and verification, decommissioning, and multi-operator closure. The remaining Universal v2.1 additions are sector-neutral and apply as written; the alignment section introduction lists them and the governing cross-references.

New challenge. Challenge 11 (The 6G Standardization Window) addresses the once-per-generation opportunity now open: 3GPP Release 19 froze in March 2026 with SA3's quantum-safe protocol inventory complete, Release 20 carries the 6G studies and an approved PQC transition study, and Release 21 will produce the first normative 6G specifications. PQC can be native in 6G where it is a retrofit in 5G, and the window to influence requirements is the study phase running now.

Currency updates. The regulatory alignment map reflects the June 2026 standards state, including the Release 19 freeze, the Release 20/21 trajectory, GSMA PQ.03 v2.0 and PQ.07 (non-terrestrial networks), and the EU coordinated roadmap dates. Further Reading was updated, and a cross-reference to the companion book, Quantum Ready, was added.

TOOL AND VENDOR REFERENCES

This framework references specific tools, products, and vendors as illustrative examples to help practitioners understand the categories of capability available. A mention does not constitute an endorsement, recommendation, or assessment of fitness for any particular environment. The PQC tooling market is evolving rapidly; products mentioned may have changed in capability, licensing, or availability since publication. Organizations should conduct their own evaluation based on their specific requirements, regulatory environment, and procurement constraints.

The body of this edition names categories and capability requirements. Commercial vendors appear in the body only where a dated public fact is itself the evidence (the three network equipment providers the Universal names as a concentration fact; the handset platforms' published PQC deployments). The references below carry the names the body relied on in the June 2026 edition, verified September 2026 only where stated, and are maintained on PQCFramework.org between editions.

Network equipment providers (sector characteristics; Challenge 7; Phase 7, Tier A): the June 2026 edition named Ericsson, Nokia, Samsung and Huawei as RAN vendors and Ciena, Nokia, Huawei, Cisco and Ericsson as transport equipment vendors. Ericsson, Nokia and Huawei stay in the body as the concentration fact the Universal states; the others describe the installed base this extension was written against and are not an assessment of any vendor's PQC readiness, which is established per product through the Phase 7 questionnaire and graded for firmness.

SIM and eUICC vendors (Challenge 6; Phase 7, Tier A): the June 2026 edition named Thales, IDEMIA and Giesecke+Devrient (G+D). PQC support in SIM hardware, secure-element firmware and eSIM profiles is established per product and per SGP specification release through the Phase 7 questionnaire; no vendor's status is asserted at this edition.

General-purpose HSMs (Phase 6): the June 2026 edition named Thales Luna, Entrust nShield and Utimaco. Thales Luna HSM firmware 7.9 (July 2025) added native ML-KEM and ML-DSA, with FIPS 140-3 Level 3 validation of that firmware in progress at release; earlier 7.8 firmware did not carry the lattice algorithms. Utimaco Quantum Protect (April 2025) is an application package for the u.trust General Purpose HSM Se-Series, activated in the field without a hardware exchange, carrying ML-KEM, ML-DSA, LMS/HSS and XMSS/XMSS-MT; older Utimaco models outside the Se-Series are a

hardware question. Entrust nShield PQC status is not verified at this edition. Each date is graded for firmness in the operator's register.

Validated modules (alignment section): CMVP certificate #5247, the Go Cryptographic Module (versions v1.0.0 and v1.0.1, Geomys LLC; a FIPS 140-3 Level 1 software module validated April 27, 2026), lists ML-KEM key generation and encapsulation-decapsulation at ML-KEM-768 and ML-KEM-1024 among its approved algorithms, not ML-KEM-512 and no ML-DSA; some validated modules still list PQC only among their non-approved services, and a listing of that kind does not count. Consult the CMVP validated-modules list for the current state.

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 Getting Started with Quantum Security and PQC Migration page: https://postquantum.com/starting-pqc-quantum-security/, 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.org, a dedicated companion site for this framework, drawing on relevant content from PostQuantum.com.

Two sibling Applied Quantum properties carry work this framework cites rather than repeats. The Applied Quantum CBOM Profile, the property taxonomy layered on CycloneDX that Phase 2 cites by minimum version, publishes at CBOMProfile.org. The Cryptographic Concentration Framework, which measures cryptographic concentration beneath the vendor layer and consumes a Profile-conforming CBOM, publishes at CCFramework.org. Both are open under CC BY 4.0 and follow this framework's sector taxonomy.

This framework is the execution methodology. For the complete treatment (the reasoning behind each phase, extended case examples, and guidance for leading the program from the first board conversation through closure), see the companion book, *Quantum Ready* (QuantumReady.com). Quantum Academy (QuantumAcademy.com), founded by the author, offers trainings and certifications on the topics this framework covers, for the roles and training levels described in Skills & Team Structure.

The PQC Migration Brief (pqcmigrationbrief.com) carries corrections, standards and regulatory movement between editions, and the current jurisdiction roster is maintained on the Global PQC Migration Clock page on PostQuantum.com; the framework itself remains free and ungated.

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 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 in Phase 1 and CBOM documentation in 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. The operator must wait for the vendor to release firmware or hardware that supports them. The same dependency applies to SIM/UICC secure elements, session border controllers, GGSN/PGW gateways, and virtually every other network component.

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 become an active, ongoing workstream from Phase 0 onward, not treated as a late-stage activity.

A small number of network equipment providers (Ericsson, Nokia and Huawei, named in the Universal's Telecommunications note as a public fact) control the cryptographic implementations across most network cores, and every date one of them gives the operator is graded for firmness under Activity 7.5 before it enters the roadmap. How many distinct cryptographic implementations, trust anchors and firmware families execute beneath those providers is the Cryptographic Concentration Framework's question (CCFramework.org). This extension cross-references it in Phases 3 and 7 and computes no concentration figure.

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 a post-quantum SUPI concealment scheme until 3GPP defines the protection scheme, its key sizes, and the protocol modifications in a formal Release. Both 5G-AKA and RAN ciphering are symmetric.

The 3GPP question for them is the move to the 256-bit algorithm sets (Challenge 11), and neither depends on a Shor-vulnerable primitive. As of September 2026, 3GPP SA3's study on the transition to post-quantum cryptography (TR 33.703, *Study on transitioning to Post Quantum Cryptography (PQC) in 3GPP*, a Release 20 study independent of any generation) is published. The 3GPP specification record holds it under change control since June 17, 2026, with version 20.0.0 approved at SA#112 and

uploaded June 25, 2026 and version 20.0.1 uploaded July 3, 2026, under work item FS_CryptoPQC (UID 1080045), with SA3 as the responsible group.

The study completed on its Release 20 schedule. A published technical report is not a deployable profile. Three things still stand between the report and a post-quantum SUCI scheme an operator can deploy: the normative work items the report feeds, the specification text that defines a protection scheme and its identifier, and the vendor and platform implementations of that text. Each of those is a date the operator does not set and grades for firmness (Activity 7.5). 3GPP expects the Release 20 specifications to freeze by mid-2027 and Release 21, the first normative 6G release, to complete no earlier than early 2029, on the timeline agreed at the June 2026 plenaries (Challenge 11).

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 (SUPI concealment; and, on the symmetric side, the 256-bit algorithm sets for 5G-AKA and 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. What the operator can technically deliver is set by its own architecture and its own keys: at the interception points its architecture defines, it delivers the intercepted content and related data that its network carries in the clear or that it can decrypt with keys it holds. Content protected end to end under keys the operator does not hold sits outside that capability, and no general duty to defeat such encryption follows from the delivery obligation itself.

What each jurisdiction actually requires is a separate question. National LI and assistance regimes differ, and some of them impose capability, assistance or design duties that reach past the architecture an operator runs today. Legal and compliance owners map the obligation per jurisdiction and per instrument, and that mapping is an input to migration planning rather than something the network diagram settles. PQC migration touches the obligation wherever it changes the keys the operator holds or the points at which content is available in the clear, and it must preserve the capabilities the mapping records, verified before the change is deployed. Few other industries carry a migration constraint of this kind.

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 separate continents, subject to different regulations, and using equipment from unrelated 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. Roaming interfaces are the hardest elements to migrate and carry the highest HNDL exposure 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

Each challenge below states its technical basis, real-world context, and the Universal Framework phases it most directly affects. The phase adaptations that follow map the challenges to the framework.

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

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.

Remediation requires a 3GPP specification update: a post-quantum protection scheme with its identifier in TS 33.501 Annex C. The update then reaches the handset population, the USIM population, or both, depending on where each subscription computes the SUCI. 3GPP TS 31.102 specifies both locations through the USIM service table (EF_UST): service 124 (subscription identifier privacy support) enables SUCI concealment, and service 125 (SUCI calculation by the USIM) selects where it is computed.

Where both services are available the USIM computes the SUCI. Where service 124 is available and service 125 is not, the mobile equipment computes it, reading the home network public key and the protection scheme identifiers from EF_SUCI_Calc_Info on the card. A subscription in mobile-equipment calculation mode therefore needs handset software that implements the new scheme and updated key material in EF_SUCI_Calc_Info, by the remote reprovisioning channel or by card replacement; only a subscription whose USIM computes the SUCI needs card-side capability for the new scheme, by replacement or by a secure-element update the card can take. An operator's own EF_UST provisioning records answer which population it faces and in what proportion, and Phase 1 inventories that split before any campaign is sized.

Framework Impact: Phase 1 (Discovery) must map all ECIES usage in SUPI concealment and record, per subscription population, whether the SUCI is computed by the mobile equipment or by the USIM (EF_UST services 124 and 125), with the count of each and the count unknown. Phase 5 (Pilots) must include SIM/eSIM reprovisioning pilots for the USIM-calculation population and a handset-software pilot for the mobile-equipment-calculation population. Phase 7 (Vendor) must track SIM vendor and handset platform PQC readiness.

Challenge 2: Radio Access Network Constrained Environments

Radio units (O-RUs in Open RAN, or proprietary RRHs), distributed units and centralized units operate on embedded processors with strict latency, power, and memory constraints. Which unit performs which cryptographic function follows the RAN functional split and the product, and not the cabinet. PDCP-layer ciphering belongs to the unit that terminates PDCP, which in a split architecture is the centralized unit, and a lower-layer radio unit does not generally own it.

Fronthaul and midhaul carriage divides the same way. An Ethernet segment is protected with MACsec where it is protected at all, and an IP segment with IPsec, so IKEv2 is assessed on the segments that actually run IPsec, and the certificate-based key distribution behind MACsec on the segments that key it from 802.1X EAP-TLS rather than from a pre-shared key (Challenge 7). The symmetric ciphers on the air interface (SNOW 3G, AES-128, ZUC) are not directly quantum-vulnerable, and the 3GPP question for them is the 256-bit algorithm sets (Challenge 11).

The quantum-vulnerable element is the public-key exchange wherever one exists, which on fronthaul and midhaul is the IKEv2 exchange (finite-field or elliptic-curve Diffie-Hellman) that establishes an IPsec tunnel. 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 control-plane network functions (AMF, SMF, NRF, UDM, AUSF, PCF and others) communicate over

HTTP/2 with mutual TLS. The UPF is not in that mesh: it sits on the user plane and is controlled by the SMF over the N4 interface, so its cryptography is inventoried with the user-plane and transport estate, not with the SBA. Which TLS version, key-exchange group and certificate profile a given inter-NF connection runs follows the 3GPP security profile the operator has deployed and the vendor build behind each network function, so Phase 1 records them per connection instead of asserting one TLS and ECDHE configuration across the mesh.

The two tracks then move on separate schedules. Track A upgrades the TLS stacks at both peers of a connection and the negotiation policy that selects the hybrid group, and its verification result is the group observed on that connection. Track B migrates certificate issuance on the NF PKI and the signature algorithms the peers accept, where the deployed profile requires it, and its verification result is the certificate signature algorithm in production.

Deploying hybrid key establishment does not by itself require the certificates to be reissued under a PQC signature algorithm, which is why the two tracks are planned, recorded and verified separately. Both tracks raise handshake and chain sizes that the Network Repository Function (NRF) and the SCP (Service Communication Proxy) have to carry.

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 over the N32 interface, which has two parts: N32-c, the connection that manages the interface and negotiates its security capability over mutually authenticated TLS, and N32-f, the connection that carries the protected messages. TS 33.501 clause 13 provides two protection modes for N32-f. Where the SEPPs connect directly, N32-f runs over TLS, with separate TLS connections for N32-c and N32-f. Where IPX providers offer only IP routing between the SEPPs, either TLS or PRINS may be used; and where IPX intermediaries need to read and modify messages in transit, PRINS (PRotocol for N32 INterconnect Security, clause 13.2) applies.

Under PRINS the SEPPs protect the N32-f message payload with JSON Web Encryption under symmetric keys agreed over the N32-c connection, and each intermediary

appends its modifications as a JSON Web Signature object that the receiving SEPP validates before applying the patch. The quantum-vulnerable asymmetric cryptography on N32 therefore sits in three places and not in the bulk of the traffic: the TLS handshakes on N32-c and, in TLS mode, on N32-f; the certificates that authenticate the SEPPs and the intermediaries; and the JWS signatures the intermediaries apply under PRINS.

The symmetric JWE protection of N32-f under PRINS is not a Shor target. Migrating N32 to PQC requires bilateral agreement between operators, aligned vendor support on both SEPPs and at every modifying IPX intermediary, and 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 3 must also record the delivery state of every roaming entry as dependent on the peer or the IPX provider that has to move with it. Phase 4 must model bilateral operator coordination timelines, with a firmness grade on every date a peer or an IPX provider supplies (Activity 7.5). Phase 7 must run roaming and interconnect peers under the counterparty pattern (Activity 7.6), with GSMA engagement for the ecosystem-wide steps; GSMA PQ.05, Quantum-safe Cryptography for 4G and 5G Roaming (July 2025), is the sector's published reference for the interfaces this challenge describes.

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 delivers, at those points, the intercepted content and related data that its own network carries in the clear or that it can decrypt with keys it holds. Content protected end to end under keys the operator does not hold is outside that technical capability.

Whether the legal obligation reaches further than the capability is a question of the national LI and assistance regime, which in some jurisdictions imposes capability, assistance or design duties, and it is mapped per jurisdiction and per instrument by legal and compliance owners before a migration plan treats it as settled. PQC migration touches the capability at three points: the key establishment the operator terminates, on which the interception point relies for content in the clear; the TLS on the LI mediation, handover and delivery interfaces themselves; and the LI key-management module (Phase 6). PQC migration must preserve the capabilities that mapping identifies

as required at all three, and each approved change is verified against them before deployment.

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 USIMs hold the home network public key and the protection scheme identifiers for SUPI concealment in EF_SUCI_Calc_Info and execute the AKA algorithm using symmetric keys; whether the card or the handset computes the SUCI is set per subscription in the USIM service table (Challenge 1). Deploying PQC-protected SUPI concealment therefore requires card-side support for the new scheme only in the USIM-calculation population, meaning new SIM hardware or secure element firmware from the SIM vendors for that population (the vendors named in the June 2026 edition are listed in the front-matter Tool and Vendor References). The mobile-equipment-calculation population needs handset software that implements the scheme and an update of the key material on the card.

The installed base of SIMs globally is measured in billions. For a single operator with 50–100 million subscribers, the card campaign covers the USIM-calculation share of that base, a share its own provisioning records state and this extension does not estimate. Replacing or reprovisioning that share is a multi-year logistics and customer-experience challenge, while the mobile-equipment-calculation share migrates with handset software and a key-material update on the card. eSIM (eUICC) technology offers remote provisioning capability, but PQC support in eSIM profiles depends on the eSIM platform vendor and the GSMA's Remote SIM Provisioning specification series (SGP), which contained no PQC provisions at the June 2026 edition; re-verify against the current SGP release before planning against it.

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; ML-KEM hybrid key exchange enabled by default in Chrome 131, Universal Activity 5.2), but enterprise MDM and VPN configurations add additional complexity.

Framework Impact: Phase 1 must inventory the subscription population by SUCI computation location, USIM profile and eSIM platform version. Phase 4 must plan the card campaign for the USIM-calculation population and the handset-software dependency for the mobile-equipment-calculation population. 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. The quantum-vulnerable element is the public-key exchange where one exists: IKEv2 on IPsec; on MACsec, the certificate-based 802.1X EAP-TLS that distributes the connectivity association key, while a link keyed from a pre-shared CAK has no public-key exchange and only a key-distribution path to record (Phase 6, Transport encryption by protocol); on OTN-layer encryption, whatever key-exchange mechanism the vendor's product implements, recorded per product.

The transport network may involve equipment from several vendors, each with its own upgrade path and PQC timeline and each date graded for firmness (the vendors named in the June 2026 edition are listed in the front-matter Tool and Vendor References).

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 now 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 all but 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.

Challenge 11: The 6G Standardization Window

5G is a PQC retrofit; 6G does not have to be. 3GPP Release 19 froze in March 2026 with SA3's inventory of the security protocols that use cryptography in the 5G system complete. Release 20 runs the 6G work as studies only (technical reports; the release also includes normative 5G-Advanced work). SA3's study on transitioning 3GPP systems

to PQC (TR 33.703), which is independent of any generation, is published: the 3GPP specification record shows it under change control since June 17, 2026, version 20.0.0 approved at SA#112 and uploaded June 25, 2026, version 20.0.1 uploaded July 3, 2026, under work item FS_CryptoPQC (UID 1080045).

It completed on its Release 20 schedule and defines the normative work packages that follow it. Completion of the report is not the arrival of a deployable scheme. The work items, the specifications and the implementations that would deliver one are what the operator tracks and grades from here. Release 20 also introduces the 256-bit algorithm sets for 5G (TS 35.240 to TS 35.248) and studies 256-bit authenticated encryption for the access and non-access strata (TR 33.771).

Release 21 produces the first normative 6G specifications on the timeline agreed at the June 2026 plenaries: package approval and Stage-1 freeze in March 2027, Stage-2 freeze in June 2028, Stage-3 freeze in December 2028, and the ASN.1 and OpenAPI freeze in March 2029. The consequence is a once-per-generation window: requirements written into the Release 20 studies determine whether 6G authentication, subscriber identity protection, and inter-network security support PQC natively from the first specification, or inherit another retrofit cycle.

Two failure modes follow from the window. Operators that disengage from SA3 and the GSMA Post-Quantum Telco Network Task Force inherit defaults set by vendors and other operators, then discover them in procurement. And operators that treat 6G as the fix defer 5G migration that cannot wait. Those 5G estates will run for a decade or more alongside 6G, and HNDL collection against them is current. The EU and national regulatory clocks (see the regulatory alignment map) do not pause for a generation change.

The GSMA PQ series, PQ.01 to PQ.07 (the impact assessment of February 2023 through the guidelines for telecom use cases of October 2024, the roaming guidance of July 2025 and the non-terrestrial-network paper of February 2026), is the operator coordination channel for both problems.

Framework Impact: Phase 0 and Phase 4 treat the 6G timeline as a planning input, not a reason to wait: the migration plan covers the 5G estate on its own clock, with 6G-native PQC as the convergence point. Phase 7 adds the Release 20 and 21 PQC items (the work packages that follow TR 33.703; the Release 21 security specifications on the agreed timeline) to vendor roadmap questionnaires now, each date graded for firmness, since RAN and core refresh cycles being specified today deliver into the 6G transition. Standards engagement (SA3, GSMA PQTN, O-RAN security) is a funded program activity with named owners, not a volunteer effort.

ALIGNMENT WITH UNIVERSAL FRAMEWORK V3.0

Universal Framework v3.0 (September 2026) is a major version. Readiness against dated obligations is the mandate; crypto-agility is the method. The PQC migration is the first exercise of a standing capability to change cryptography on a planned date. For an operator, whose estate is vendor-supplied, standards-bound and shared with peers it cannot compel, the version changes the method, the records and the vendor governance, corrects published positions in the open and updates the standards the core and transport text cites.

- **Method.** The charter states both outcomes (Phase 0). The program runs ten workstreams, with Discovery separated from the permanent Cryptographic Record and Crypto-Agility funded from Year 1 (Activity 0.3). Every migration gate and wave exit applies the agility criterion, and a system whose algorithm cannot be changed by configuration and rehearsed with rollback is recorded as migrated with agility debt (Activities 4.6 and 5.4).

Every wave includes an algorithm-change rehearsal (Activity 5.2). Closure requires a rehearsed second algorithm change per track inside the agility window (the 48-hour assessment plus the organization's change window, ten business days by default) and zero unaccepted agility debt (Migration Verification & Program Closure). Phase 3 produces an agility-debt register, which in an operator's estate is filled by the standards-bound and peer-bound interfaces.

- **Records and evidence.** Every discovery finding carries an evidence grade E1 to E5; coverage is measured against a denominator enumerated before discovery runs. The accepted-gaps register is signed at gate G1 → G2 (Activity 1.2). The CBOM minimum record is the Universal's own (Activity 2.1), with the Applied Quantum CBOM Profile v1.0-RC or later cited as informative carriage and never required. The Cryptographic Concentration Framework is cross-referenced where the question is

how many distinct implementations execute beneath the network equipment providers (Activity 3.1). No concentration figure is computed in this extension.

- **Vendor governance.** Every roadmap date is graded for firmness (committed, forecast, announced, unknown). The questionnaire opens with the two agility questions and the firmness question; four certificate-authority questions and the non-standardized-algorithm rule with its one-afternoon test apply (Activities 7.2, 7.3 and 7.5). Counterparties the operator cannot compel, which in telecommunications are the roaming and interconnect peers, the IPX providers and the standards bodies, follow Activity 7.6; cloud-hosted network functions follow Activity 7.7.
- **Corrections made in the open.**

On HNDL. HNDL is stated as inference from demonstrated capability, never as observed harvesting. The July 2026 PostQuantum.com analysis in Further Reading sets out why the harvest itself cannot be observed.

On validated modules. The Universal's June 2026 statement that no validated module offered approved PQC was wrong when published (CMVP certificate #5247, April 2026). Validation is decided per product, per operation and per certificate (Deployment Environment Classification).

Six statements in the June 2026 edition of this extension are corrected. Three are matters of citation and method:

- It attached a version suffix to PQ.03 that the GSMA's document list does not show. The series is PQ.01 to PQ.07, with PQ.03 dated October 2024.
- It scored risk on a five-dimension model that the Universal had already replaced with four (Phase 3).
- Its regulatory map merged NIST IR 8547's 2030 and 2035 dates into a CNSA 2.0 row. The two instruments are separate rows of the Universal's roster.

Three changed what the edition recommended.

On SIM reprovisioning it said that remediation "requires both a 3GPP specification update and a SIM replacement or remote reprovisioning campaign affecting every subscriber."

3GPP TS 31.102 specifies both mobile-equipment and USIM calculation of the SUCI, selected per subscription by EF_UST services 124 and 125. The population needing a new or reprovisioned card is therefore the one whose USIM computes the SUCI itself. An operator that sized a campaign against the published text re-reads its own EF_UST provisioning records and splits the estate. The mobile-equipment population migrates with handset software and updated key material in EF_SUCI_Calc_Info. Only the USIM-calculation population needs a card replacement or a secure-element update (Challenge 1, Phase 1).

On the roaming interface it listed "N32/SEPP roaming interfaces" under Track A beside subscriber-facing TLS and NF-to-NF TLS, and did not distinguish the two protection modes.

TS 33.501 clause 13 provides both: TLS where the SEPPs connect directly, and PRINS where IPX intermediaries read and modify messages. Under PRINS the N32-f payload is protected by symmetric JWE under keys agreed on the N32-c connection. The asymmetric dependency therefore sits in the N32-c and TLS-mode N32-f handshakes, in the certificates, and in the JWS signatures the intermediaries apply (Challenge 4).

On the service-based architecture it said that migrating the mesh to PQC-protected TLS "requires updating every network function's TLS stack, reissuing certificates with PQC algorithms."

Key exchange and authentication are separate mechanisms in TLS 1.3, which is why this framework runs two tracks. Deploying hybrid key establishment does not by itself require certificates to be reissued under a PQC signature algorithm, and a complete authentication migration is Track B scope with its own verification result (Challenge 3).

Standards currency runs to September 2026: RFC 9954 and RFC 10024 for hybrid TLS, with X25519MLKEM768 registered Recommended=Y and the pre-standard Kyber768 code points obsoleted; RFC 9370 for hybrid IKEv2; RFC 10042 for hybrid SSH; resumption protected by mode; and the section 8 conditions of SP 800-208 on the deploy-now firmware-signing action. The 3GPP and GSMA items are dated in Challenge 11 and in the Regulatory Alignment Map.

The subsections below read each element for operator estates. The last three read elements the June 2026 edition did not cover (the agility criterion and rehearsal; evidence grades and the coverage denominator; vendor dates and questions). The remaining Universal positions apply as written, with three notes. The counterparty coordination pattern in Activity 7.6 maps directly onto the telecom interconnect problem: roaming and interconnect partners number in the hundreds, offer no contractual leverage beyond GSMA frameworks, and must move in concert, so the pattern's dual-stack windows, deprecation protocol, and interoperability test events apply to roaming and IPX migration without adaptation.

The cloud shared-responsibility treatment in Activity 7.7 applies wherever network functions run on public cloud, with the boundary-verification requirement (observed negotiation, not provider blog posts) applied at the operator-to-cloud seam. And crisis communications (GRC) operates at subscriber scale: a quantum cryptographic event at an operator triggers mass-market notification and regulator timelines simultaneously, so the pre-drafted templates are a program prerequisite, not a documentation exercise.

Two-Track Migration Model in Telecommunications

Track A (Confidentiality / Key Exchange): subscriber-facing TLS, service-based architecture NF-to-NF TLS inside the 5G core, N32/SEPP roaming interfaces (the N32-c handshake and, in TLS mode, the N32-f connection; Challenge 4), IPsec backhaul and transport encryption, and management-plane VPNs. This track addresses HNDL against subscriber data and signaling, where collection interest is permanent and the lawful-interception adjacency raises the stakes.

Track B (Integrity / Signatures / PKI): network function certificates and the internal PKI behind them; OAuth token signing in the SBA; network element and RAN firmware signing; eSIM profile signing; and OSS/BSS code signing. SUCI subscriber-identity concealment sits with Track A's key-establishment problem (it is an ECIES construction), while the AKA root credential K is symmetric and comparatively quantum-resilient at adequate key length. The asymmetric wrappers around subscriber identity, not the AKA core, require the migration.

Validation Decided Per Product in Carrier Infrastructure

Under the Universal Framework's Deployment Environment Classification, validation is decided per product, per operation and per certificate. The classification keys on the module certificate rather than on the configuration.

The Universal's June 2026 statement that no validated module offered approved PQC was wrong when published. CMVP certificate #5247, the Go Cryptographic Module (versions v1.0.0 and v1.0.1, Geomys LLC), is a FIPS 140-3 Level 1 software module validated on April 27, 2026. Its approved algorithms include ML-KEM key generation and encapsulation-decapsulation at ML-KEM-768 and ML-KEM-1024, not ML-KEM-512, and no ML-DSA. The Go module version that implements ML-DSA is on the Modules In Process list and not on the validated list.

Some validated modules still list PQC only among their non-approved services, and a listing of that kind does not count.

Most of an operator's estate classifies as unrestricted or FIPS-aware. Hybrid key exchange on the management plane, OSS/BSS, SBA TLS and the roaming edge therefore proceeds now on mainstream library support, with any documented risk acceptance recorded per system.

The constraint binds upstream. The modules inside carrier-grade equipment, and the HSMs behind SIM personalization and certificate issuance, are validated by their vendors product by product. Record the certificate that covers each PQC operation, its status and its tested environment in the Phase 6 register, and ask for them in the Phase 7 questionnaire.

Operators serving government customers inherit FIPS-required obligations on those slices of the estate, as written. Three examples are a government slice, a dedicated enterprise VPN service, and a lawful-interception delivery path. Where a contract or a regulation places one of these in the FIPS-required class, it runs PQC only through a module whose certificate lists the operation as an approved service, and its production date is set from that certificate.

Classify per the Universal model. The FIPS-required population must not delay hybrid deployment on the unrestricted majority of the estate.

Merkle Tree Certificates and Operator Web Estates

The Universal position on Merkle Tree Certificates concerns the public Web PKI, and it touches operators at two points. Customer-facing web properties and public APIs follow the browser ecosystem's fork on the browser ecosystem's schedule (the Chrome Quantum-resistant Root Store is targeted for Q3 2027 and Let's Encrypt chose Merkle Tree Certificates on June 3, 2026; Universal Phase 6, PKI Architecture Evolution), at the certificate volumes a mass-market subscriber base implies.

The internal telco PKI (NF certificates, SBA TLS, device management) is operator-controlled and follows the operator's plan, not the MTC trajectory. Its constraint is the certificate-lifecycle automation needed at telecom scale, which this extension's PKI material addresses. Track the two estates separately.

Hybrid and Composite Signatures in Network Infrastructure

The Universal Framework's default (Activity 5.2) is composite or dual signatures, with solo ML-DSA recorded as a risk decision. The hedge exists only where the verifier requires both signatures. The verifier acceptance policy is recorded with the format. In operator estates the default holds for NF certificates, OSS/BSS code signing, and network element firmware (dual-signed), and the 3GPP and GSMA direction for transport favors hybrid key establishment, which is consistent.

The default breaks at the constrained edge: SIM applet signatures, legacy RAN elements, and length-limited protocol fields may not carry composite structures. Record those as documented solo decisions per the Universal position, with the implementation-maturity exposure weighed explicitly and compensating monitoring on the affected interfaces. A constrained population that can carry no post-quantum signature at all is protected at the nearest gateway under the OT & Critical Infrastructure Extension's Encapsulate strategy, with the enclosure boundary stated in the CBOM.

Algorithm Weighting in the ECC-Heavy 5G Core

The Universal's weighting position (Activity 3.1: quantum attack cost tracks key size, not classical strength, and the 2026 resource estimates moved the 256-bit-curve figures

while the RSA figures held) applies directly to 5G. SUCI subscriber-identity concealment runs on ECIES profiles over P-256 or Curve25519, SBA TLS authenticates with ECDSA certificates, and the modern core is ECC-heavy precisely because ECC is efficient. At equal criticality, weight the ECC-based 5G core at least as early as legacy RSA-based OSS/BSS, and note that subscriber identity has one of the longest confidentiality horizons an operator holds: a harvested SUCI exchange decrypted later exposes who was where, retroactively, for the archive's full depth.

Subscriber and Network Identity in Track B

The Universal's identity and authentication scope in Track B translates in telecom to two estates. Subscriber identity: the AKA root key K is symmetric and holds at adequate length. The asymmetric mechanisms around it split by cryptographic function, as the Universal's routing rule requires (Activity 3.3). SUCI concealment is key establishment, ECIES encrypting the SUPI to the home network's public key, and it is a Track A entry whose protected data is the confidentiality of the subscriber's identity; eSIM profile signing under the GSMA specifications and device attestation are signatures and are Track B entries.

Network and operational identity: NF certificates and the internal CA hierarchy, OAuth 2.0 token signing inside the SBA, TLS client certificates on management interfaces, and federation with enterprise and wholesale customers. The network estate and the signing part of the subscriber estate are Track B entries and SUCI concealment is a Track A entry. The SIM/eSIM ecosystem constraints in Challenge 6 set the replacement physics for the subscriber side of both.

SP 800-208 for Network Element and eSIM Firmware Signing

The Universal makes SP 800-208 stateful hash-based signatures the deploy-now component of Track B under the conditions of section 8 of that publication: key and signature generation inside a hardware module with at least Level 3 physical security, no export of the private key in any form, and signing state managed inside the module so that backup, replication and failover designs cannot reuse a state. A signing service that does not meet section 8 is not a conforming deployment, and the verifiers in the field must accept the parameter set chosen.

The operator's version of deploy-now runs through vendors: RAN and core element firmware signing migrates at the network equipment provider. The procurement requirement (LMS/XMSS-signed firmware with verifier support, and a statement of how the vendor's signing service meets section 8) belongs in every refresh-cycle RFP now. The eSIM and eUICC profile-signing ecosystem is GSMA-governed; track its PQC trajectory through the PQTN task force and the SGP specification series rather than waiting for it to arrive in a vendor brochure.

The state-management condition argues for HSM-backed signing services on both the vendor and operator side. The operator's own signing module records its certificate reference and entropy validation in the Phase 6 register.

Securing the CBOM as a Network Map

Universal Activity 2.5 treats the CBOM as a high-value intelligence target, and the telecom CBOM is among the most sensitive instances anywhere: a complete cryptographic inventory of an operator exposes core topology, roaming and interconnect architecture, and the placement of LI touchpoints. LI-adjacent entries may be subject to legal handling constraints of their own in several jurisdictions. Partition the CBOM by domain, restrict LI-adjacent records to the cleared population that already handles them, log every read, and design SOC integration with role-based access controls so that automated feeds do not expose the full inventory to the broader organization.

When a regulator, a lawful-interception authority, an auditor or a roaming peer asks for the CBOM, the Universal's rule applies: attest, do not send. In place of the document, the requester gets a signed commitment to the snapshot, a coverage statement with its denominator and method, and the predicate it needs (Activity 2.5).

Verification, Decommissioning, and Multi-Operator Closure

The Universal's Migration Verification & Program Closure section defines the evidence standard for declaring a system migrated and the closure criteria: a verification disposition for every Tier-1 and Tier-2 service in one of four states (migrated; migrated with agility debt and a funded closure date; enclosed or compensated under an accepted exception; retired), the closure proof, and the agility-debt register at zero unaccepted debt.

In telecommunications the standard meets a boundary the operator does not own: it cannot unilaterally declare a shared interface closed. Verification on roaming and interconnect runs on observed negotiation at the IPX and SEPP boundaries. Classical-suite retirement on those interfaces follows the counterparty pattern (Activity 7.6): published dual-stack windows, a T-minus deprecation protocol communicated through both commercial and technical channels (with GSMA coordination where the change is ecosystem-wide), and documented residual-risk acceptance for partners that lag.

A shared interface the peer cannot change on the operator's date exits its wave as migrated with agility debt, with the peer, the peer's date and that date's firmness grade in the register entry. An interface whose peer has refused to move requires either the refusal decision of Activity 7.6 as an accepted exception signed by the SteerCo or documented residual-risk acceptance; without one of those records, the interface remains open.

Closure is read against the roaming and interconnect population and not only the operator's own estate: every Tier-1 and Tier-2 roaming, interconnect and standards-bound entry has a disposition, and the register reaches zero unaccepted debt when every remaining entry has a funded treatment with a date (a peer's committed date, a 3GPP normative release with its own date and grade, a vendor release) or a SteerCo-signed exception.

The closure proof runs where the operator controls the change: for Track A, the hybrid-group change on the SEPP and on the management plane; for Track B, the certificate-signature-algorithm change on the NF issuing CA, each inside the agility window and minuted with the segment timings. Inside the operator's own estate the standard evidence applies, including decommissioning of legacy signaling-era key material where interconnect dependencies permit.

The Agility Criterion and Rehearsal in Telecommunications

The Universal's agility criterion (Activity 4.6) asks four things of a migrated system: the negotiated outcome observed, classical-only refused and tested where policy requires it, the algorithm changeable by configuration, and a rehearsal in staging with the rollback exercised. An operator's estate splits on the third and fourth conditions by who owns the change. On the layers the operator configures (management-plane SSH and TLS, OSS/BSS interfaces, the SBA TLS policy distributed to the network functions, the SEPP's N32 configuration, the internal NF PKI and the transport VPN concentrators) all four conditions are met by the operator's own change.

On the layers a standard or a peer owns, the recorded state follows the protection result, which is what the first two conditions decide. A roaming interface whose peer has accepted the hybrid group has passed them, and it is the third and fourth conditions that wait for the peer: that entry is recorded as migrated with agility debt against the peer's graded date. SUCI concealment in the USIM or the handset and in the UDM has not passed them, because there is no post-quantum protection scheme for the operator to negotiate until 3GPP publishes one and it reaches the handset software or the card.

That entry is blocked rather than migrated with agility debt: it stays in its wave with its exposure recorded and its bridging pattern named (Phase 3). The 256-bit algorithm sets for 5G-AKA and RAN ciphering are a third case, because those populations are symmetric and have no Shor exposure. Nothing waits there on a protection result, and what the register carries against the 3GPP date is the operator's inability to change the algorithm set on a date of its own.

This extension states the sector's agility objective in those terms: an operator is crypto-agile when it can change the algorithm on the layers it controls on a planned date and can state the graded target for every standards-bound or peer-bound interface. Every wave includes an algorithm-change rehearsal on the layer the wave touches, timed across assessment, decision, change and verification with the rollback exercised: a

hybrid-group change on the SEPP's N32 interface against a lab peer, a parameter-set change on the management-plane TLS policy, a certificate-signature-algorithm change on the NF issuing CA against a staging core.

The rehearsal never runs against a live roaming partner or a live lawful-interception path. Where a change touches the interception architecture, the decision segment includes the regulator's approval step and the recorded window includes it (Challenge 5). A rehearsal that cannot be scheduled because the change waits for a 3GPP release, a vendor firmware release, a SIM campaign or a peer has found agility debt before production did. The entry goes to the Phase 3 register with its treatment and its date.

Evidence Grades and the Coverage Denominator in Telecommunications

Every discovery finding is assigned an evidence grade in the Universal's five tiers (Activity 1.2): E1, runtime observed; E2, binary confirmed; E3, inventory declared; E4, vendor attested; E5, inferred. In an operator's estate the grades follow the ownership boundaries. Passive monitoring at the SEPP, the IPX edge, the management plane and inside the SBA produces E1 for the key-exchange groups it sees. The certificate inventory and the NF PKI produce E2 and E3 for Track B. The RAN, the SIM population and the transport equipment produce E4 (a vendor's questionnaire answer or firmware catalog entry) and E5 (a capability inferred from a 3GPP profile or a product manual).

The grade attaches to the claim, not to the row: the entry for a base station's IPsec module can have E1 for the key-exchange group observed on the backhaul and E4 for the firmware version the vendor states. A Tier-1 entry known only at E4 or E5 requires verification before it warrants funding, and a vendor statement about a future release grades the date (Activity 7.5), never the finding. Coverage is measured against a denominator enumerated before discovery runs: the network element inventory and the site database, the NF catalog and the NRF's registration data, the roaming agreement register and the IPX contracts, the SIM logistics and eSIM platform records, the OSS/BSS application catalog and the transport link database.

A scope derived from what the monitoring tools happened to observe does not qualify. Populations the method cannot observe (SIM applet cryptography, ciphering inside the radio unit, traffic inside a peer's network, interception paths the operator is not cleared to inspect) are named as unobserved, with coverage unknown rather than zero. The accepted-gaps register signed at gate G1 → G2 by the Discovery lead, the CISO and the SteerCo records the scope the denominator contains and discovery did not reach, with the reason and a planned closure date. In an operator that register is long by design. It is a governance artifact.

Vendor Dates and Questions in Telecommunications

Every date in this extension's tables, dependency maps and vendor scorecards is graded under the Universal's four firmness grades (Activity 7.5): committed (contractual, with

remedies), forecast (a planning date stated in writing), announced (a public roadmap statement) or unknown. Phase 3 Dimension 3 scores the grade, independent of the calendar date. In telecommunications the grade applies to three kinds of date the operator does not set: a network equipment provider's firmware release; a standards body's freeze or publication, where a 3GPP timeline is announced until the release freezes and a GSMA document date is a publication and not a commitment; and a peer's or an IPX provider's migration date, which is unknown until the peer states it in writing under the counterparty pattern.

The questionnaire opens with the two agility questions and the firmness question (Activity 7.2); for network equipment, the second agility question, whether the product's verifiers and trust stores can be updated in the field, decides whether a firmware-signing or certificate change reaches deployed radio units and transport nodes without a site visit. The four certificate-authority questions apply to the operator's NF PKI provider, to every equipment vendor operating its own CA for device certificates, and to the eSIM ecosystem's certificate issuers as the GSMA governs them.

The non-standardized-algorithm rule and its one-afternoon test (Activity 7.3) apply to any "quantum-safe" claim made in transport, RAN or SIM products under a proprietary or pre-standard algorithm: public specification with test vectors, public cryptanalysis by parties other than its designers, a standards-body track, a validated or CAVP-tested implementation. A product that fails the first two tests is excluded from approved-mode use, with the sovereignty caveat for a national algorithm mandated under a documented regime. Every roadmap date in Phase 4 and Phase 7 is graded; Phase 3 scores the grade.

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 requirement types that bind the operator (Universal, Deadline Archetypes): the plan-by and migrate-by dates of the EU coordinated roadmap and NIS2 for operators that are essential entities; the transition-plan requirements that national telecom regulators now issue, which set a plan-by date where a regulator has issued one; the CNSA 2.0 networking-equipment date inherited through government-customer contracts; and the GSMA post-quantum guidelines, which set no date.

The argument is not "regulators require PQC today" but "the regulatory trajectory makes PQC investment inevitable: early movers face lower costs and less disruption." The sector bodies and their status are in this extension's Regulatory Alignment Map. The jurisdiction roster is in the Universal's Regulatory Timeline Context and on the Global PQC Migration Clock page.

- **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. The evidence dossier is what the customer's due diligence asks for.
- **The dual-outcome charter:** State both outcomes in the charter in the operator's terms (Universal Activity 0.4): readiness against the operator's dated obligations (the EU roadmap's end-2030 date for high-risk use cases where the operator is an essential entity, the national telecom regulator's transition-plan requirement where one has issued, the government-customer contracts that impose CNSA 2.0 or FIPS-required terms, the lawful-interception approvals) as the mandate, and the standing capability to change cryptography on the layers the operator controls on a planned date, with a graded date for every standards-bound and peer-bound interface, as the end state. The agility-debt register, populated by those interfaces, is part of the readiness evidence.

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, the approvals a regulator attaches to changes in the interception architecture (Challenge 5), and national security reporting requirements.

Two owners are named in the charter beside the SteerCo (Universal Activity 0.3). In an operator the Crypto-Agility workstream owner belongs to the network engineering function that owns the SBA TLS policy, the SEPP configuration and the NF PKI, and not to security alone. The Cryptographic Record owner keeps the telecom CBOM after the discovery project ends. The three lines are stated by function: the program under the CISO and the CTO is first line and delivers. The risk function is second line and challenges the scoring model, the gate decisions and closure; internal audit is third line. The board approves the risk appetite and receives the KPI pack.

Phase 1 – Discovery & Inventory

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), each recorded with the functions it actually performs: where PDCP-layer ciphering terminates, where an IPsec tunnel terminates and where MACsec does, and whether each fronthaul and midhaul segment is carried over Ethernet or over IP.

Record the MACsec or IPsec profile in force on each segment and the key-distribution path behind it, so that IKE is assessed on the segments running IPsec and the 802.1X EAP-TLS path on the segments keying MACsec from a certificate (Challenge 7). Record the cryptographic acceleration each platform provides, by product and by algorithm, with the post-quantum operations it does and does not support. A general statement that no post-quantum acceleration exists is not an inventory finding, and Phase 6 benchmarks what this track names.

- **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, with the N32-f protection mode per peer (TLS, or PRINS with each modifying IPX intermediary named), so that a TLS-mode peer is recorded as the N32-c and N32-f handshakes and a PRINS-mode peer as the N32-c handshake plus a signature entry per intermediary (Challenge 4). SS7/Diameter security proxy configurations. IPX provider security capabilities.
- **SIM/device inventory track:** Subscription populations by USIM vendor and profile, with the SUCI computation location read from the USIM service table (EF_UST service 124 present with service 125 present: USIM calculation; service 124 present and service 125 absent: mobile-equipment calculation), the ECIES protection scheme and key profile held in EF_SUCI_Calc_Info, the eUICC population with its SGP platform versions, and the count of subscriptions for which the location is unknown.

Card form factor (2FF, 3FF, 4FF) is a mechanical attribute that does not determine cryptographic capability and is recorded for logistics only. Device population by OS version and PQC capability, since the mobile-equipment-calculation population migrates with the handset software (Challenge 1).

- **OSS/BSS inventory track:** Application catalog with TLS configurations, certificate dependencies, database encryption methods, and vendor support status.

Every finding on these tracks is tagged with its evidence grade (the alignment section's evidence subsection): E1 for a key-exchange group observed at the SEPP, the IPX edge,

the management plane or inside the SBA, E2 for a binary or firmware image analyzed, E3 for an NF catalog, NRF registration or configuration export, E4 for a vendor's questionnaire answer or firmware catalog entry, and E5 for a capability inferred from a 3GPP profile or a product manual.

Each track states its denominator before discovery runs (the site database, the NF catalog, the transport link database, the roaming agreement register, the SIM logistics records, the OSS/BSS application catalog). What the denominator contains and discovery did not reach goes to the accepted-gaps register signed at G1 → G2.

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) and, in the same pass, the SUCI computation location per subscription population (a read of the provisioning records, not a network scan, and the fact that sizes the SIM campaign), 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 model: CBOM Layer 1 (the TLS, SSH and IPsec configurations on the SEPP, the transport nodes, the management plane and the NF mesh) and CBOM Layer 2 (the NF PKI, the HSMs, the SBA's OAuth issuer) first, so that which protocol on which interface uses which algorithm class is recorded before implementation-level detail; CBOM Layer 4 (the RAN, SIM and transport firmware the operator cannot open) is populated from vendor disclosure and graded accordingly.

The record is the Universal's own minimum record (Activity 2.1), with the evidence grade on every claim and the five fields marked recorded at Phase 3 (trust scope, verifier updatability, dependency firmness, compensating controls, delivery state) recorded on every entry for the scoring run to populate. Organizations that structure the CBOM under the Applied Quantum CBOM Profile, v1.0-RC or later, record the same fields as Profile properties. The Profile is informative carriage and never required.

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." The tag maps onto the entry's delivery state in Phase 3 (Activity 3.2): operator-controlled reads as available; vendor-dependent as dependent on a graded release date; standards-dependent as dependent on a 3GPP release date or blocked until one exists.

Phase 3 – Risk Scoring & Prioritization

Adapted Risk Scoring Model

The Universal's four dimensions (Activity 3.1) stand: Dimension 1, data sensitivity and exposure (HNDL risk); Dimension 2, trust infrastructure criticality (TNFL risk); Dimension 3, migration feasibility; Dimension 4, regulatory and compliance pressure. The June 2026 edition of this extension scored on a five-dimension list taken from the 2025 model. That list is withdrawn. The telecommunications adaptation adds no dimension.

It restates the two additions of earlier editions as factors inside Dimension 3 and uses the Universal's arithmetic (Activity 3.2): Low = 1 to Critical = 4, and Easy = 1 to Hard = 3 on the inverted feasibility dimension. A dimension scores the highest of its factors; an inapplicable dimension is excluded with the weights renormalized; an unknown value is left unscored, listed and resolved before the entry is tiered.

- **Standards dependency (the Universal's protocol-maturity factor inside Dimension 3, read for the sector):** The cryptography changes by operator configuration under a standard that already specifies PQC (TLS, SSH and IPsec on the management plane, OSS/BSS, the SBA and transport) = Easy; the standard exists and the change waits on a vendor release for the network element (RAN IPsec, transport encryption, NF software) = Medium; no 3GPP, O-RAN Alliance or GSMA specification yet specifies the change (SUCI concealment, the SIM applet, eSIM profile signing; and, on the symmetric side, the 256-bit algorithm sets for 5G-AKA and RAN ciphering, which are a key-length question and not a Shor exposure) = Hard. A Hard entry is dependent or blocked on a standards date with its firmness grade. It keeps the tier the ordered test gives it and is listed in the agility-debt register.
- **Multi-operator coordination (the Universal's interoperability-constraints factor inside Dimension 3, read for the sector):** Internal to the operator = Easy; bilateral,

with one roaming partner or one IPX provider = Medium; multilateral, across the roaming ecosystem or an IPX community = Hard. A roaming or interconnect entry is dependent on its peers whatever its score. The peer's date and its grade are recorded in the entry.

- **Weighting:** The Universal's default weights stand (HNDL 0.35, TNFL 0.25, regulatory 0.25, feasibility 0.15). The SteerCo ratifies the weights and the appeals rule before the first scoring run (Activity 0.3). Dimension 1's accessibility factor is scored against a state-level collector, so a flow that crosses an IPX, a submarine cable or a satellite link scores as partner-facing at least, and the air interface, open to any collector in radio range, scores as internet-facing.

Dimension 4 reads the enforcement tier of the instrument that binds the entry (Regulatory Alignment Map). Verifier updatability, the Universal's Dimension 2 factor, is read per entry: a burned-in trust anchor in a radio unit, a transport node or a SIM applet is Critical and is the strongest single indicator of agility debt in the estate. A centrally managed NF trust store is Low.

Algorithm-specific weighting: Apply the Universal's vulnerability weighting (Activity 3.1) in operator scoring: quantum attack cost tracks key size rather than classical strength, so the ECC-heavy 5G core (SUCI, SBA certificates) weighs at least as urgent as legacy RSA-based OSS/BSS at equal criticality. See the alignment section's Algorithm Weighting subsection.

Telecommunications Priority Tiers

Priority	System Category	Rationale	Typical Delivery State
Tier 1	International interconnect (N32 in both modes, IPX and transit links, legacy SS7/Diameter interconnect where a key exchange exists); every internet-facing entry (subscriber portals and APIs, application backends, internet-facing management and vendor remote-access gateways); SUCI concealment over the air interface;	Placed by the ordered test of Activity 3.2: Dimension 1 Critical with accessibility High or Critical (an internet-facing entry; a partner-facing flow carrying subscriber identity, location or content whose horizon exceeds 15 years; the air interface, scored as internet-facing under the Weighting bullet above); or Dimension	Available on the operator's side for the SEPP, the internet-facing services, the management gateways and the internal PKI; dependent on each peer for the shared N32 interface and on the vendor for radio-unit, transport-node and device anchors, shown against the date with its firmness grade; blocked for

Priority	System Category	Rationale	Typical Delivery State
	leased-circuit, microwave and satellite transport segments carrying traffic with a horizon over 15 years; the NF PKI root and every network-wide trust anchor; firmware-signing, secure-boot and certificate-issuer anchors in radio units, transport nodes, eUICCs, SIM applets and device fleets where the verifier cannot be updated in the field	2 Critical on any factor (a root or network-wide trust anchor, 15 years or more of verification, verifiers that cannot be updated); or Dimension 4 Critical (a mandatory deadline within 2 years under a tier 1 to 3 instrument; none of this map's rows has one at this edition, and a government slice inherits CNSA 2.0's dates through the Universal's roster and its contract).	SUCI concealment until the 3GPP protection scheme exists and reaches the handset software or the card. A blocked entry names its bridging pattern on the record (below)
Tier 2	Core network SBA mesh (inter-NF TLS, OAuth token signing, NF certificates under a shared intermediate); transport encryption on operator-owned fiber (IPsec, MACsec, OTN, fronthaul and midhaul IPsec) and on leased circuits carrying traffic with a horizon of 15 years or under; internal management-plane TLS and SSH; OSS/BSS with subscriber data on internal interfaces; PKI intermediates;	Dimension 1 Critical or High with internal accessibility (subscriber data and topology carry horizons over 15 years, but an internal flow does not meet the first condition), unless the entry is air-gapped; or Dimension 2 High (a shared intermediate, a key several network functions or external parties rely on, verifiers updatable by campaign, 5 to under 15 years of verification); or Dimension 4 High (a	Available for the OSS/BSS, management-plane and PKI entries the operator configures; dependent on a vendor release with a firmness grade for the NF software, the transport nodes and the RAN elements

Priority	System Category	Rationale	Typical Delivery State
	government slices and enterprise services under a contract that requires PQC; entries under a mandatory deadline within five years once the NIS2 transposition or a national telecom regulator's instrument reaches enforcement tier 2 or 3	mandatory deadline within 5 years, or a contract that requires PQC).	
Tier 3	Entries whose highest applicable dimension is Medium: internal flows and stores carrying data with a horizon of over 5 to 10 years (operational telemetry and analytics, non-subscriber network data), single-application signing keys verified by centrally managed trust stores within one system, IoT and M2M segments on private APNs carrying data with that horizon on devices whose trust stores update by campaign, entries under a general regulatory expectation only	Any applicable risk dimension (1, 2 or 4) Medium or above, and none High or Critical. Plan now; execute in the roadmap's later waves.	Available, dependent or blocked as the record states; the delivery state moves the roadmap date and never the tier

Priority	System Category	Rationale	Typical Delivery State
Tier 4	Entries whose every applicable risk dimension is Low: an internal or air-gapped entry carrying data with a horizon of 5 years or under, with no signature role beyond one session or process and no regulatory expectation attached. Few operator entries meet the condition	Every applicable risk dimension Low. Monitor; compensating controls; migrate when feasible. A blocked migration does not place an entry here: IoT and M2M fleets that cannot be updated, legacy 2G/3G infrastructure and satellite backhaul are tiered on their risk above, take the delivery state blocked, and run under compensating controls (segmentation, overlay encryption at the aggregation point) as their bridging pattern	Blocked entries are shown in the tier the ordered test gives them, not in this one

Delivery state and the agility-debt register. Delivery state is the field of Activity 3.2 with four values: available, dependent, blocked, unknown. A blocked entry retains the tier the ordered test gives it regardless of the block, and the composite score orders entries inside a tier and never assigns one. The entry appears on the roadmap against its unblocking date, which in an operator is a 3GPP release, a vendor firmware release with a firmness grade, a handset platform release, a SIM campaign or a peer's committed date.

Dependent is the common state for the standards-bound layers, and a SUCI entry blocked on 3GPP stays in Tier 1. A blocked Tier-1 entry names its bridging pattern on the record. For a Track A flow, the pattern is the overlay of Activity 7.4 where one can wrap the flow: a PQC-capable IPsec concentrator ahead of a satellite or microwave hop, or the operator's own hybrid negotiation on N32-c with classical acceptance recorded per peer under the dual-stack windows of Activity 7.6.

For SUCI concealment no overlay exists because the scheme runs end to end between the subscriber's equipment and the home network. A blocked SUCI entry names Activity 7.4's documented residual-risk acceptance with the 3GPP release as the re-evaluation trigger, the HNDL-exposure determination of Activity 1.1 recording what a harvested SUCI exchange yields once decrypted (the subscriber's permanent identifier, at the place and time of the recorded registration), and the standards engagement of Challenge 11.

For a non-updatable verifier population, the pattern is the campaign or replacement plan with its date, or the same documented acceptance. The telecom estate fills the agility-debt register with the entries a standards body or a peer owns: every Tier-1 and Tier-2 entry scored Hard on standards dependency or multi-operator coordination, or Critical on verifier updatability, is listed with the reason (standards-bound algorithm, non-updatable verifier, vendor-locked configuration, peer-bound interface). The entries are derived from the scores already recorded and add no dimension (Activity 3.1).

Phase 4 – Roadmap & Governance

External Dependency Mapping

Telecommunications roadmaps must explicitly model three categories of external dependency that most enterprises do not face, and every date recorded under them has a firmness grade (committed, forecast, announced, unknown; Activity 7.5) that Phase 3 scores in place of the calendar date:

- **Standards-body timelines:** 3GPP Release schedules for PQC-enabled specifications (Release 20's transition study and its normative work packages; the Release 21 freezes agreed in June 2026, Challenge 11), O-RAN Alliance security specification updates, and GSMA post-quantum guideline evolution. A standards date is announced until the release freezes, and a study completion date is not a specification date.
- **Vendor delivery timelines:** Per-vendor PQC firmware and software release dates for each major equipment category (RAN, core, transport, SIM), each graded, tracked as external milestones in the program plan, and re-baselined under Activity 4.8 when a committed date slips past the bridging capacity recorded in Activity 7.4.
- **Inter-operator coordination timelines:** Bilateral roaming agreement updates and GSMA-coordinated migration windows for interconnect protocols. A peer's date is unknown until the peer states it in writing under the counterparty pattern (Activity 7.6), and a lawful-interception approval that a change requires is a dependency with the regulator's date, graded like any other (Challenge 5).

Gates, Recorded States and Re-Baselining

Every gate record from G5 → G6 onward, and every wave-exit record, shows two results as separate fields (Universal Activities 4.6 and 5.4): the protection result (which

interfaces and boundaries are verified, which remain exposed) and the agility result (which change was rehearsed, through which mechanism, in what elapsed time). An interface can pass on protection because the operator's side negotiated the hybrid group and the peer accepted it.

If it cannot change its algorithm on the operator's date because the peer or the standard owns the change, it exits the wave as migrated with agility debt, with the entry and its closure date in the Phase 3 register. The two results are independent. Blocked Tier-1 and Tier-2 entries keep their tier and appear on the roadmap against their unblocking dates. The Re-Baseline Protocol (Activity 4.8) governs every committed date that depends on a party the operator does not control: a network equipment provider slipping a committed firmware date beyond the bridging capacity recorded in Activity 7.4, a 3GPP freeze moving, a roaming peer missing its stated date, or a lawful-interception approval arriving late opens a re-baseline review at the next SteerCo, minuted to the evidence dossier. A slipped date that is not re-baselined tells the regulator that the program has lost control of its schedule.

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. Name the Crypto-Agility workstream owner and the Cryptographic Record owner. Issue PQC readiness RFIs to the top-5 network equipment vendors, agility questions first, and grade every date returned. Begin LI regulatory pre-engagement.
- **Q2:** Complete the Tier-1 cryptographic inventory (interconnect, the internet-facing services and management access, the PKI roots and the burned-in anchors, and the SUCI computation location per subscription population) with evidence grades and the denominator stated. Begin OSS/BSS TLS migration pilots. Rehearse an algorithm change on the management-plane pilot, timed and rolled back.
- **Q3:** Complete core network SBA CBOM. Record the delivery state of every scored entry and open the agility-debt register. 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 and the first agility KPI reading. 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 key exchange: mlkem768x25519-sha256 for SSH per RFC 10042 (the default in current OpenSSH) and X25519MLKEM768 for TLS per RFC 10024. Low risk, high learning value, operator-controlled, and the first rehearsal target.
- **Pilot 2 – OSS/BSS inter-system TLS:** Select 2–3 internal BSS application interfaces and deploy X25519MLKEM768 (hybrid ML-KEM-768 with X25519; RFC 9954 for the framework, RFC 10024 for the named group). Measure latency and compatibility.
- **Pilot 3 – Transport IPsec:** Deploy hybrid IKEv2 (RFC 9370, the Universal's Appendix H row for IPsec) on a non-production transport segment (a lab or disaster-recovery link). Test MTU behavior, fragmentation, and middlebox compatibility.
- **Pilot 4 – Core network NF mesh:** In a lab or staging 5G core, set X25519MLKEM768 as the SBA's TLS group policy and migrate inter-NF TLS to it. Benchmark control-plane call-setup latency under load, and force a fresh handshake on the persistent NF sessions after enablement (below).
- **Pilot 5 – SEPP/roaming (coordinated):** Bilateral pilot with a willing roaming partner to test X25519MLKEM768 on the N32-c TLS connection and, in TLS mode, on the N32-f TLS connection between SEPPs. Where the peer runs PRINS, the pilot verifies that the N32-f JWE session keys derive from a hybrid N32-c handshake and inventories the JWS signatures of each modifying IPX intermediary as a separate Track B surface (Challenge 4).

GSMA PQ.05 (Quantum-safe Cryptography for 4G and 5G Roaming, July 2025) and PQ.06 (Implementation and Prototype Verification of Post-Quantum Use Case: Hybrid Key Exchange, May 2026) are the sector's published references for the pilot. The pilot follows the counterparty pattern (Activity 7.6) and requires GSMA coordination where the change is ecosystem-wide.

Resumption, long-lived sessions and pre-standard code points. The persistent TLS sessions of the NF mesh, the SEPP's N32 connections and the management-plane sessions are long-lived channels in the Universal's sense (Activity 5.2). A session established with classical key exchange and kept alive is unaffected by a hybrid capability enabled later. Resumption is protected by mode and not by the age of the ticket. Pilot design forces a fresh handshake on a defined interval after hybrid enablement, requires the hybrid group on resumption (psk_dhe_ke with X25519MLKEM768), disables PSK-only resumption and 0-RTT for the flows in scope, and may expire pre-migration tickets as the simpler policy; TLS 1.3 KeyUpdate creates no post-quantum secret and is not a substitute.

A pilot that ran in 2023 or 2024 on the draft X25519Kyber768Draft00 or SecP256r1Kyber768Draft00 code points retires them on a dated schedule (RFC 10024 obsoletes them at Recommended=D), verified by a negative test that no draft group is offered or negotiated on any production SEPP, network function or management endpoint. The test is repeated at verification.

Rehearsal per wave and the wave-exit criterion. Every wave, from the management plane outward, includes an algorithm-change rehearsal on at least one system in the wave, timed across assessment, decision, change and verification with the rollback exercised (Universal Activity 5.2). In an operator the rehearsal target is the layer the wave touches and the operator configures: the management-plane TLS policy, the SBA group policy in the staging core, the SEPP's N32 configuration against a lab peer, the NF issuing CA.

Each wave exit applies the agility criterion (Activity 4.6): negotiated outcome observed, classical-only refused and tested where policy requires it, algorithm changeable by configuration, change rehearsed with rollback. A shared interface that meets the first two conditions and cannot meet the last two on the operator's date exits as migrated with agility debt, with the peer's or the standard's date and grade recorded. The wave-exit record shows the protection result and the agility result separately.

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 a structural requirement in telecom, not a design preference.

The dual stack on roaming and interconnect is a permanent operating state that requires governance: record the deprecation date for classical acceptance per peer and per interface, test the refusal where policy requires it, and report the classical-only population as its own line in the KPI supplement.

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:** X25519MLKEM768 adds 1,184 bytes of ML-KEM-768 encapsulation key to the ClientHello and 1,088 bytes of ciphertext to the ServerHello (Universal Activity 6.3). In a dense SBA mesh with thousands of connections, test aggregate impact on control-plane throughput and session-establishment latency.
- **Certificate chain bloat:** An ML-DSA-65 signature is 3,309 bytes and its public key 1,952 bytes, against about 64 bytes of signature for ECDSA P-256 (Universal Appendix A), so a certificate chain grows by an order of magnitude. Test impact on OCSP/CRL checking overhead, especially for short-lived NF certificates.

- **Fronthaul bandwidth:** Test hybrid IKEv2 (RFC 9370) overhead on bandwidth-constrained eCPRI fronthaul links. Determine whether PQC handshake sizes require MTU adjustments or fragmentation handling.
- **Transport encryption by protocol:** IPsec backhaul migrates through hybrid IKEv2 (RFC 9370), which the Universal's Appendix H lists as deployable now. Appendix H has no MACsec row: a MACsec link keyed from 802.1X EAP-TLS follows the Universal's 802.1X row and migrates with the TLS stack and the internal PKI, and a link keyed from a pre-shared connectivity association key has no public-key exchange to migrate, so its CBOM entry records the key distribution path instead. OTN-layer encryption follows its vendor's key-exchange mechanism, recorded per product.
- **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 the HSM vendors early on their PQC roadmaps and certification timelines (FIPS 140-3, Common Criteria) and grade every date. The products named in the June 2026 edition are listed in the front-matter Tool and Vendor References. The operator's HSM and KMS register records the Universal's four fields (Activity 6.2): the visible platform, the supplier's firmware family, the manufacturer of origin and the FIPS 140-3 certificate reference, plus the entropy references (the SP 800-90B validation as an ESV certificate reference or the ENT designation on the module certificate, with the operating envelope).

Three rows are always present: the SIM personalization and key-transport module; the NF issuing CA's key store; and the lawful-interception key-management module, whose row records the handling constraints of Activity 2.5. A firmware-signing module for the operator's own images records its conformance to section 8 of SP 800-208 against its certificate (the alignment section).

Phase 7 – Vendor & Supply Chain Governance

Telecommunications Vendor Classification

Classify vendors by their impact on PQC migration timeline. The number of vendors does not equal the number of distinct cryptographic dependencies: whether two RAN vendors, or a RAN vendor and a transport vendor, execute one cryptographic implementation family is the Cryptographic Concentration Framework's question. That question is cross-referenced from the vendor register and never computed here.

- **Tier A – Timeline-blocking:** The network equipment providers of the RAN and the core (the three named in the sector characteristics as a public fact; the wider list the

June 2026 edition named is in the front-matter Tool and Vendor References), the SIM vendors (also listed there), and the core network software vendors. These vendors' PQC readiness directly determines when the operator can migrate specific network layers. Engage at CTO-to-CTO level. Every date they give is graded for firmness.

- **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.

Questionnaire Order, Certificate-Authority Questions and the One-Afternoon Test

The questionnaire opens with the two agility questions and the firmness question (Universal Activity 7.2). For network equipment the second agility question is asked for the installed base: can the verifiers and trust stores of deployed radio units, transport nodes and SIMs be updated in the field, by what mechanism, and without a site visit or a SIM swap. The four certificate-authority questions (ML-DSA and FN-DSA end-entity issuance dates; hybrid or composite issuance; the public Web PKI roadmap where a customer portal or an API chains to public roots; the date the issuer's own signing keys become PQC-capable and how the root transition reaches relying network functions and devices) are asked of the operator's NF PKI provider, of every equipment vendor operating its own CA for device certificates, and of the eSIM ecosystem's certificate issuers as the GSMA governs them.

Any product that carries a public-key algorithm not standardized by NIST or an equivalent national authority is disclosed and run through the one-afternoon test (Activity 7.3). A proprietary "quantum-safe" claim in a transport, RAN or SIM product that fails the first two tests is excluded from approved-mode use, with the sovereignty caveat for a national algorithm mandated under a documented regime. For cloud-hosted network functions the two-part roadmap ask of Activity 7.7 (the negotiated state per service today, observable at the boundary, and the dated targets for each, graded) goes into the same questionnaire. Every roadmap date in this section and in the vendor scorecard is graded for firmness; Phase 3 scores the grade.

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 Telco Network Task Force:** Coordinates operator-to-operator migration planning, roaming interface PQC guidelines, and SIM ecosystem PQC requirements; publishes the PQ series, PQ.01 to PQ.07, as listed on the GSMA's document page in September 2026: PQ.01 Post Quantum Telco Network Impact Assessment (February 2023), PQ.02 Guidelines for Quantum Risk Management for Telco (September 2023), PQ.03 Guidelines for Telecom Use Cases (October 2024), PQ.04 Post Quantum Cryptography in IoT Ecosystem (February 2025), PQ.05 Quantum-safe Cryptography for 4G and 5G Roaming (July 2025), PQ.06 Implementation and Prototype Verification of Post-Quantum Use Case: Hybrid Key Exchange (May 2026) and PQ.07 Post Quantum Cryptography for Non-Terrestrial Networks (February 2026).
- **O-RAN Alliance Security Focus Group:** Defines security specifications for Open RAN, including PQC requirements for disaggregated RAN components.
- **ETSI TC CYBER QSC:** Publishes the migration guidance the Universal's front matter cites (TR 103 619, migration strategies and recommendations, July 2020; TR 104 016, a repeatable framework for quantum-safe migrations, October 2024) and the quantum-safe hybrid key-exchange specification TS 103 744 (December 2020), all applicable to European telecom operators and read by their regulators.
- **National telecom regulators:** Pre-engage on LI implications, critical infrastructure PQC mandates, and compliance timelines.

TELECOMMUNICATIONS REGULATORY ALIGNMENT MAP

The rows below are the sector's own bodies and instruments as of September 2026, each with its status and with the enforcement tier the Universal's Regulatory & Standards Alignment Map assigns (tier 1, market access; tier 2, supervisory directive with a named enforcer; tier 3, binding government mandate with an audit trail; tier 4, authoritative guidance; tier 5, advisory). The jurisdiction roster in the Universal (NIST IR 8547, CNSA 2.0, the EU coordinated roadmap, NCSC UK, Australia, Canada) is not repeated here: it is in the Universal's Regulatory Timeline Context and, kept current between editions, on the Global PQC Migration Clock page.

Two rows of that roster reach operators through channels the map does not repeat: CNSA 2.0's networking-equipment date (2030) binds the government slices an operator serves through contract, and NIST IR 8547's 2030 and 2035 dates, still a draft at this edition, are the reference the sector's instruments cite. National telecom regulators now issue transition-plan requirements. A regulator that sets a plan-by or migrate-by date for operators is a row on the Clock page, and it enters this map only where the date is verified against the instrument.

The June 2026 edition's row for national critical-infrastructure regulators, which cited a French target that is not telecom-specific, is replaced by that pointer. Every date is re-checked against its instrument at each release, and readers verify status and applicability for their own jurisdiction before planning against a row.

Instrument	Requirement and Dates	Status at This Edition (Enforcement Tier)	Telecom Implication
EU NIS2 and the NIS Cooperation Group coordinated roadmap	Essential entities implement state-of-the-art security	Roadmap published June 2025; COM(2026) 13	Telecom operators are essential entities. Plan the interconnect,

Instrument	Requirement and Dates	Status at This Edition (Enforcement Tier)	Telecom Implication
	measures (NIS2); Member States plan and execute the PQC transition (roadmap). National strategies by end-2026; high-risk use cases by end-2030; the remainder by end-2035	(January 20, 2026) proposes PQC as a named NIS2 obligation and is not adopted at this edition (tier 4, hardening to tier 2 or 3 through national transposition and supervision)	core and management-plane estate to the 2030 date; the transposing law and the national telecom regulator are where the entity-level obligation lands.
3GPP SA3	PQC integration in 5G-Advanced and 6G security specifications. Release 19 frozen March 2026 with the cryptographic-protocol inventory complete; Release 20 study on the transition to PQC (TR 33.703) published and under change control since June 17, 2026 (version 20.0.0 approved at SA#112 and uploaded June 25, 2026; version 20.0.1 uploaded July 3, 2026; work item FS_CryptoPQC, UID 1080045), with the 256-bit algorithm sets (TS 35.240 to TS 35.248) and the 256-bit AEAD study (TR 33.771); Release 20 freeze expected mid-2027; Release 21, the first normative 6G release, on the	Report published and under change control per the 3GPP specification record; the normative work items, the specifications and the implementations a deployable PQC profile needs are still ahead of it (tier 4 for the published specifications; tier 5 for the report)	The normative work that follows the report sets when operators can deploy a standards-compliant post-quantum SUCI scheme and the 256-bit algorithm sets for 5G-AKA and RAN ciphering, and when the 3GPP cryptographic profiles for SBA TLS and N32 are revised; until a protection scheme publishes and reaches the handset software or the card, the SUCI entries stay blocked, and the profiled protocols migrate by configuration where the standard already permits the hybrid group.

Instrument	Requirement and Dates	Status at This Edition (Enforcement Tier)	Telecom Implication
	timeline agreed June 2026 (Stage-1 freeze March 2027; Stage-3 freeze December 2028; ASN.1 and OpenAPI freeze March 2029)		
GSMA Post-Quantum Telco Network Task Force, PQ.01 to PQ.07	Impact assessment (PQ.01, February 2023), risk management (PQ.02, September 2023), telecom use cases and migration (PQ.03, October 2024), IoT (PQ.04, February 2025), 4G and 5G roaming (PQ.05, July 2025), hybrid key-exchange prototype verification (PQ.06, May 2026), non-terrestrial networks (PQ.07, February 2026); no dates set	Published series, as listed on the GSMA document page in September 2026 (tier 5)	Non-binding and industry-coordinating: the algorithm preferences, the roaming migration guidance and the coordination channel for the dual-stack windows of Activity 7.6.
ETSI TC CYBER QSC	Migration strategies and recommendations (TR 103 619, July 2020), a repeatable framework for quantum-safe migrations (TR 104 016, October 2024), quantum-safe hybrid key exchanges (TS 103 744, December 2020); no dates set	Published (tier 5)	Migration guidance European operators and their regulators read; the Universal's Appendix G crosswalks TR 103 619 to this framework.

Instrument	Requirement and Dates	Status at This Edition (Enforcement Tier)	Telecom Implication
O-RAN Alliance	Security specifications for disaggregated RAN	Not re-checked since the June 2026 edition: ongoing updates, no PQC parameter cited (tier 5)	Defines PQC requirements for multi-vendor RAN as they publish; affects Open RAN adopters specifically (Challenge 10).

TELECOM MATURITY MODEL SUPPLEMENT

The levels, names and descriptions are the Universal's single 0 to 5 scale (Maturity Levels), used by the enterprise model and every per-phase table alike. The sector indicators are read beside them, and the closure criterion reads the same scale.

Level	Universal Name and Description	Telecom-Specific Indicator
0	Unaware: no organizational awareness of quantum cryptographic risk; no activities planned or underway	No sector indicator.
1	Aware: quantum risk acknowledged at leadership level; initial education conducted; no formal program	CISO/CTO joint sponsorship. 3GPP SA3 participation initiated. LI regulatory pre-engagement begun. Which instruments bind the operator (essential-entity status under NIS2, government-customer contracts, a national telecom regulator's requirement where issued) identified.
2	Initiated: formal program chartered; budget allocated; discovery underway; initial CBOM in development	Charter states both outcomes; Crypto-Agility and Cryptographic Record owners named. Tier-1 (interconnect, internet-facing services, PKI roots and burned-in anchors, SUCI computation location) inventory complete with evidence grades and a stated denominator. Core SBA

Level	Universal Name and Description	Telecom-Specific Indicator
		CBOM initiated. SIM inventory by vendor, profile and SUCI computation location (EF_UST services 124 and 125). RAN hardware capability baseline. Roaming agreement register enumerated as a denominator.
3	Progressing: CBOM operational; risk scoring complete; hybrid pilots in production; vendor engagement active; KPIs reported	Scoring model ratified with the telecom factors; agility-debt register produced, with the standards-bound and peer-bound populations listed. Multi-track roadmap (operator-controlled, vendor-dependent, standards-dependent) approved with a firmness grade on every external date. SIM vendor and RAN vendor PQC timelines integrated and graded. LI compliance plan reviewed by regulators. First algorithm-change rehearsal run on the management-plane pilot. Agility questions first in every new RFP.
4	Advanced: Tier-1 systems migrated to hybrid/PQC; PKI modernized; crypto-agility demonstrated; vendor commitments secured	Tier-1 systems on the layers the operator controls pass the protection result at their gates: the hybrid group negotiated at the SEPP and on the management plane and accepted by the peer, observed. Each shared interface that fails the configuration or rehearsal conditions on the operator's date is recorded as migrated

Level	Universal Name and Description	Telecom-Specific Indicator
		with agility debt against the peer's graded date, and the blocked Tier-1 populations (SUCI concealment, the non-updatable anchors) run under their named bridging pattern with the residual exposure recorded. Core SBA TLS migration underway, two results in every wave-exit record. Transport encryption PQC rollout in progress. GSMA roaming PQC coordination active with published dual-stack windows. An algorithm change rehearsed on the SEPP and on the NF issuing CA inside the agility window. Tier A vendor dates graded, with committed dates for core and transport firmware.
5	Optimized: estate-wide PQC migration substantially complete; crypto-agility is organizational capability; continuous monitoring and posture management operational	Full network PQC coverage on the layers the operator controls, with compensating controls for the standards-dependent layers under SteerCo-signed exceptions. Crypto-agile architecture embedded in the NF lifecycle. CBOM maintained across all domains by the Cryptographic Record owner. Roaming interfaces pass the protection result on both sides of N32 (the hybrid group negotiated with the peer and accepted by it, or the PRINS session keyed from a hybrid N32-c handshake), and each that cannot change

Level	Universal Name and Description	Telecom-Specific Indicator
		its algorithm on the operator's date is recorded as migrated with agility debt against the peer's committed date. Standing rehearsal cadence on the SEPP, the management plane and the NF PKI. Agility-debt register at zero unaccepted debt: every remaining standards-bound or peer-bound entry funded with a date or under a SteerCo-signed exception.

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 the enumerated denominator (Phase 1) with a graded cryptographic finding, reported per domain (RAN, core, transport, OSS/BSS, interconnect, SIM and device) with the known population count, the unknown population from the accepted-gaps register and the populations named as unobserved shown separately. A count of domains declared complete is not a coverage figure.
- **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:** The subscription population by SUCI computation location, as three counts (mobile equipment, USIM, unknown), and, once a post-quantum protection scheme exists, the percentage of the USIM-calculation population on PQC-capable cards or eSIM profiles and of the mobile-equipment-calculation population on handset software that implements the scheme.
- **Transport PQC rollout:** Number of transport encryption endpoints migrated to hybrid PQC / total endpoints.

- **Classical-only acceptance:** Roaming and interconnect interfaces on which the SEPP or the IPX edge still accepts classical-only peers, each with its recorded deprecation date (Phase 5, the dual stack).

Agility KPIs (CISO cascade, monthly; summarized to leadership under the Agility KPI)

The four agility KPIs of the Universal (Metrics, KPIs & Reporting) are measured on the layers the operator changes. The interconnect HNDL exposure KPI above stays the sector's urgency metric and is reported beside them.

KPI	Telecommunications Measurement	Threshold
Configuration-driven share	Percentage of Tier-1 and Tier-2 systems on the layers the operator configures (the SEPP and its N32 policy, the management plane, OSS/BSS interfaces, the SBA TLS policy, the NF PKI, the transport concentrators) whose key-establishment and signature algorithms change by configuration, verified by rehearsal; the standards-bound population (SUCI concealment, the SIM applet, and the symmetric 5G-AKA and RAN ciphering entries that await the 256-bit algorithm sets) and the peer-bound interfaces are reported on their own lines and never enter the numerator	Target by year from the roadmap's agility milestones (Activity 4.2); a year missed by more than 10 points triggers Crypto-Agility workstream review
Rehearsed time-to-change	Elapsed time across assessment, decision, change and verification on the most recent rehearsal, per track: for Track A the hybrid-group swap on the SEPP against a lab peer or on the management-plane policy; for Track B the certificate-	Inside the agility window; a decision segment that includes a lawful-interception approval is recorded with that approval's elapsed time, and a rehearsal whose change segment waits for a 3GPP release, a vendor release or a peer has found

KPI	Telecommunications Measurement	Threshold
	signature-algorithm change on the NF issuing CA, with the NF certificates re-issued by configuration (Activity 5.2)	agility debt, recorded in the register and not as a variance
Agility-debt burn-down	Entries closed on the Phase 3 register per quarter, with the standards-bound population as one denominator and the peer-bound roaming and interconnect interfaces as another, reported side by side	Any quarter with no reduction triggers workstream review; before closure every remaining entry has a funded treatment with a date (a 3GPP release, a vendor release, a peer's committed date) or a SteerCo-signed exception
New-system agility compliance	Percentage of new network element, NF and OSS/BSS procurements whose RFP and contract include the two agility questions, the firmness question and the crypto-agility clause with its acceptance-test rehearsal (Activity 7.3), and percentage of new NF deployments passing the CI/CD crypto-policy check	Below 95% in any quarter triggers procurement and architecture governance review

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 the cryptographic inventory immediately on the entries the ordered test places first.** Focus on international interconnect (SEPP, IPX), the internet-facing subscriber and management surfaces, the management plane (SSH, TLS on NMS/EMS), the PKI roots, and OSS/BSS with subscriber data. Read the SUCI computation location per subscription population from the provisioning records in the same pass. The operator-controlled entries among them can be inventoried and migrated without waiting for 3GPP or vendors. Record the evidence grade of each finding and the delivery state of each entry.
- **3. Issue PQC readiness RFIs to the top network equipment vendors, agility questions first.** Ask: can the algorithms be changed by configuration, and can deployed verifiers and trust stores be updated in the field. Then ask, for each product line, the date of PQC-capable firmware and whether that date is committed, forecast or announced; which algorithms; whether hybrid mode is available. Document the responses, grade every date, and integrate them 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 X25519MLKEM768 TLS (RFC 10024) and hybrid SSH (RFC 10042) 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 by SUCI computation location and initiate SIM vendor discussions.** Read the USIM service table per profile to establish which subscriptions compute the SUCI on the card and which on the handset, what eSIM penetration exists, and what your SIM vendors' PQC roadmaps look like. The card campaign for the USIM-calculation population will be the longest-lead-time activity for SUPI concealment protection, and its size is a fact in your provisioning records rather than an assumption about every subscriber.
- **8. Name a Crypto-Agility owner in network engineering.** Give the workstream an owner in the function that controls the SBA TLS policy, the SEPP configuration and the NF PKI, a budget line from Year 1, and the agility-debt register as its scope. The register will be filled by the standards-bound and peer-bound interfaces.
- **9. Schedule the first rehearsal on the management-plane pilot.** Change the TLS group policy by configuration, time the four segments, roll it back, and file the timings; then repeat the hybrid-group swap on a lab SEPP against a lab peer. The result is the first agility KPI reading and the first entry in the closure evidence.

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/

Why HNDL Cannot Be Detected (July 2026 analysis) – https://postquantum.com/post-quantum/cannot-detect-harvest-now-decrypt-later/ – The reasoning behind the framework's HNDL position: inference from demonstrated capability, and why the harvest itself cannot be observed.

The Global PQC Migration Clock – https://postquantum.com/pqc-migration-timelines/global-pqc-migration-clock/ – The maintained jurisdiction roster that this extension's regulatory map points to, including the national telecom regulators that set a date.

NIS2, DORA, and the EU Post-Quantum Roadmap – https://postquantum.com/quantum-policies/nis2-dora-pqc-quantum/ – The EU

regulatory chain from the coordinated roadmap to entity-level obligations, which reaches operators as essential entities.

The EU Just Proposed Including Post-Quantum Cryptography (PQC) in NIS2 – https://postquantum.com/security-pqc/eu-pqc-nis2/ – COM(2026) 13 and the chain from the coordinated roadmap to entity-level obligations.

Quantum Ready (companion book) – https://quantumready.com – The executive and governance dimensions of quantum readiness, complementing this framework's technical methodology.

APPENDIX J: REQUIREMENTS REGISTER

This register is generated from the text of this edition at each build and lists every statement in this extension that uses *must*. The four program-level provisions of the Universal Framework's Normative Convention bind this extension through its parent and are listed in the Universal's Appendix J; they are not repeated here. Every statement below binds inside the section that states it, and a statement that appears here without its section's conditions is read with them. The appendix letter matches the Universal's, so "Appendix J" names the requirements register in every document of the set.

Statements in document order

1. *Why Telecommunications Requires a Sector Extension, Extreme Vendor Dependency.* The operator must wait for the vendor to release firmware or hardware that supports them.
2. *Why Telecommunications Requires a Sector Extension, Extreme Vendor Dependency.* The Universal Framework's Phase 7 (Vendor & Supply Chain) must become an active, ongoing workstream from Phase 0 onward, not treated as a late-stage activity.
3. *Why Telecommunications Requires a Sector Extension, The 3GPP Standards Bottleneck.* 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 (SUPI concealment; and, on the symmetric side, the 256-bit algorithm sets for 5G-AKA and RAN ciphering).
4. *Why Telecommunications Requires a Sector Extension, Massive Physical Footprint and Long Equipment Lifecycles.* Phase 6 (Infrastructure & Performance) must include a hardware capability assessment that is far more granular than what most enterprises require.
5. *Why Telecommunications Requires a Sector Extension, Lawful Interception and National Security Obligations.* PQC migration touches the obligation wherever it changes the keys the operator holds or the points at which content is available in the clear, and it must preserve the capabilities the mapping records, verified before the change is deployed.

6. *Why Telecommunications Requires a Sector Extension, Lawful Interception and National Security Obligations.* In some jurisdictions, regulators must approve changes to LI architecture before they are deployed.

7. *Why Telecommunications Requires a Sector Extension, Lawful Interception and National Security Obligations.* This regulatory dependency adds timeline risk that must be explicitly modeled in Phase 4 (Roadmap & Governance).

8. *Why Telecommunications Requires a Sector Extension, Convergence of IT, OT, and Network Technology.* PQC migration must span all three domains simultaneously, each with different change management processes, risk tolerances, and vendor landscapes.

9. *Industry-Specific Challenges, Challenge 1: SUPI Concealment Quantum Vulnerability and the Symmetric 5G-AKA Core.* Framework Impact: Phase 1 (Discovery) must map all ECIES usage in SUPI concealment and record, per subscription population, whether the SUCI is computed by the mobile equipment or by the USIM (EF_UST services 124 and 125), with the count of each and the count unknown.

10. *Industry-Specific Challenges, Challenge 1: SUPI Concealment Quantum Vulnerability and the Symmetric 5G-AKA Core.* Phase 5 (Pilots) must include SIM/eSIM reprovisioning pilots for the USIM-calculation population and a handset-software pilot for the mobile-equipment-calculation population.

11. *Industry-Specific Challenges, Challenge 1: SUPI Concealment Quantum Vulnerability and the Symmetric 5G-AKA Core.* Phase 7 (Vendor) must track SIM vendor and handset platform PQC readiness.

12. *Industry-Specific Challenges, Challenge 2: Radio Access Network Constrained Environments.* Framework Impact: Phase 1 must include RAN hardware capability assessment (processor, memory, firmware version).

13. *Industry-Specific Challenges, Challenge 2: Radio Access Network Constrained Environments.* Phase 6 must model handshake-size impacts on fronthaul bandwidth.

14. *Industry-Specific Challenges, Challenge 2: Radio Access Network Constrained Environments.* Phase 4 must sequence RAN upgrades across the cell-site estate.

15. *Industry-Specific Challenges, Challenge 3: Core Network Service-Based Architecture Complexity.* 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.

16. *Industry-Specific Challenges, Challenge 3: Core Network Service-Based Architecture Complexity.* Framework Impact: Phase 2 (CBOM) must document every NF-to-NF TLS configuration.

17. *Industry-Specific Challenges, Challenge 3: Core Network Service-Based Architecture Complexity.* Phase 5 must include SBA-wide PQC-TLS pilot.

18. *Industry-Specific Challenges, Challenge 3: Core Network Service-Based Architecture Complexity.* Phase 6 must benchmark control-plane latency with PQC handshakes under realistic load.

19. *Industry-Specific Challenges, Challenge 4: Inter-Operator Security and Roaming Interfaces.* Framework Impact: Phase 3 (Risk Scoring) must weight roaming interfaces for HNDL exposure on international transit.

20. *Industry-Specific Challenges, Challenge 4: Inter-Operator Security and Roaming Interfaces.* Phase 3 must also record the delivery state of every roaming entry as dependent on the peer or the IPX provider that has to move with it.

21. *Industry-Specific Challenges, Challenge 4: Inter-Operator Security and Roaming Interfaces.* Phase 4 must model bilateral operator coordination timelines, with a firmness grade on every date a peer or an IPX provider supplies (Activity 7.5).

22. *Industry-Specific Challenges, Challenge 4: Inter-Operator Security and Roaming Interfaces.* Phase 7 must run roaming and interconnect peers under the counterparty pattern (Activity 7.6), with GSMA engagement for the ecosystem-wide steps; GSMA PQ.05, Quantum-safe Cryptography for 4G and 5G Roaming (July 2025), is the sector's published reference for the interfaces this challenge describes.

23. *Industry-Specific Challenges, Challenge 5: Lawful Interception Architecture Dependencies.* PQC migration must preserve the capabilities that mapping identifies as required at all three, and each approved change is verified against them before deployment.

24. *Industry-Specific Challenges, Challenge 5: Lawful Interception Architecture Dependencies.* In some cases, regulators must review and approve changes to LI architecture before network-wide deployment.

25. *Industry-Specific Challenges, Challenge 5: Lawful Interception Architecture Dependencies.* Framework Impact: Phase 0 must include LI regulatory engagement.

26. *Industry-Specific Challenges, Challenge 5: Lawful Interception Architecture Dependencies.* Phase 4 must incorporate LI compliance checkpoints.

27. *Industry-Specific Challenges, Challenge 5: Lawful Interception Architecture Dependencies.* Phase 5 must verify LI functionality in PQC pilot environments.

28. *Industry-Specific Challenges, Challenge 6: SIM/eSIM and Device Ecosystem Constraints.* On the device side, handset operating systems (Android, iOS) must support PQC in their TLS stacks for data connections.

29. *Industry-Specific Challenges, Challenge 6: SIM/eSIM and Device Ecosystem Constraints.* Framework Impact: Phase 1 must inventory the subscription population by SUCI computation location, USIM profile and eSIM platform version.

30. *Industry-Specific Challenges, Challenge 6: SIM/eSIM and Device Ecosystem Constraints.* Phase 4 must plan the card campaign for the USIM-calculation population and the handset-software dependency for the mobile-equipment-calculation population.

31. *Industry-Specific Challenges, Challenge 6: SIM/eSIM and Device Ecosystem Constraints.* Phase 7 must track SIM vendor and device OEM PQC roadmaps.

32. *Industry-Specific Challenges, Challenge 7: Transport and Backhaul Network Scale.* Framework Impact: Phase 1 must inventory transport encryption endpoints.

33. *Industry-Specific Challenges, Challenge 7: Transport and Backhaul Network Scale.* Phase 6 must benchmark PQC handshake overhead on bandwidth-constrained links.

34. *Industry-Specific Challenges, Challenge 7: Transport and Backhaul Network Scale.* Phase 7 must coordinate across transport equipment vendors.

35. *Industry-Specific Challenges, Challenge 9: IoT/M2M and Private Network Exposure.* Framework Impact: Phase 1 must inventory IoT/M2M device populations and capabilities.

36. *Industry-Specific Challenges, Challenge 9: IoT/M2M and Private Network Exposure.* Phase 3 must score IoT segments for HNDL risk.

37. *Industry-Specific Challenges, Challenge 9: IoT/M2M and Private Network Exposure.* Phase 7 must address private network customer coordination.

38. *Industry-Specific Challenges, Challenge 10: Open RAN Multi-Vendor Cryptographic Fragmentation.* The O-RAN Alliance's security specifications must also evolve to support PQC, adding another standards-body dependency alongside 3GPP.

39. *Industry-Specific Challenges, Challenge 10: Open RAN Multi-Vendor Cryptographic Fragmentation.* Framework Impact: Phase 2 must produce per-component CBOMs across the Open RAN stack.

40. *Industry-Specific Challenges, Challenge 10: Open RAN Multi-Vendor Cryptographic Fragmentation.* Phase 5 must include multi-vendor PQC interoperability testing.

41. *Industry-Specific Challenges, Challenge 10: Open RAN Multi-Vendor Cryptographic Fragmentation.* Phase 7 must coordinate across O-RAN Alliance members.

42. *Alignment with Universal Framework v3.0.* The counterparty coordination pattern in Activity 7.6 maps directly onto the telecom interconnect problem: roaming and interconnect partners number in the hundreds, offer no contractual leverage beyond GSMA frameworks, and must move in concert, so the pattern's dual-stack windows, deprecation protocol, and interoperability test events apply to roaming and IPX migration without adaptation.

43. *Alignment with Universal Framework v3.0, Validation Decided Per Product in Carrier Infrastructure.* The FIPS-required population must not delay hybrid deployment on the unrestricted majority of the estate.

44. *Alignment with Universal Framework v3.0, SP 800-208 for Network Element and eSIM Firmware Signing.* A signing service that does not meet section 8 is not a

conforming deployment, and the verifiers in the field must accept the parameter set chosen.

45. *Phase 0 adaptation, Governance Adaptation.* 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.

46. *Phase 1 adaptation, Telecom-Specific Inventory Tracks.* The Universal Framework's discovery methodology must be extended with parallel inventory tracks specific to telecommunications:

47. *Phase 4 adaptation, External Dependency Mapping.* Telecommunications roadmaps must explicitly model three categories of external dependency that most enterprises do not face, and every date recorded under them has a firmness grade (committed, forecast, announced, unknown; Activity 7.5) that Phase 3 scores in place of the calendar date:

48. *Phase 5 adaptation, Telecommunications Pilot Targets.* Telecom pilots must address the unique multi-layer, multi-vendor nature of the network.

49. *Phase 5 adaptation, The Hybrid Architecture Reality.* 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).

50. *Phase 6 adaptation, Network Impact Assessment.* PQC introduces measurable performance impacts that must be tested across the telecom-specific infrastructure:

51. *Phase 6 adaptation, HSM and Key Management Modernization.* These HSMs must support PQC algorithms.

52. *Phase 7 adaptation, Industry Coordination Forums.* Telecom operators must actively participate in industry forums that influence PQC standardization and coordination:

ABOUT

ABOUT THE AUTHOR

Marin Ivezic is a former Fortune Global 500 CISO/CTO, the founder and CEO of Applied Quantum, and the founder of Quantum Academy (QuantumAcademy.com). PostQuantum.com is his personal blog. 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.

QUANTUM READY: THE COMPANION BOOK

Quantum Ready (QuantumReady.com) is the book-length companion to this framework, written by the same author. Where this document is deliberately methodology-grade (prerequisites, activities, outputs, decision logic), the book provides the complete treatment: the reasoning behind each phase, extended case examples from real migration programs, sector narratives, and guidance for leading the program from the first board conversation through closure. The two are maintained in alignment: the framework is updated as standards, products and deadlines change, and the book supplies the depth that a methodology document omits by design.

QUANTUM ACADEMY

Quantum Academy (QuantumAcademy.com), founded by the author, offers trainings and certifications on the topics this framework covers, from executive education on quantum risk to practitioner courses on PQC migration, crypto-agility and cryptographic inventory, for the roles and training levels described in Skills & Team Structure.

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