MEXICO AND THE POST-QUANTUM TRANSITION 2026

Public evidence, attribution, and observable post-quantum maturity

Mexico analytical panel · 50 units · Codebook v1.0

Evidence cutoff: September 2, 2026

Factual review cutoff: September 18, 2026

CENTRAL FINDING

Cryptographic dependencies relevant to an eventual transition are widely observable. Local organizational post-quantum transition still cannot be estimated with sufficient coverage from public evidence.

ABOUT THE STUDY

Research report · 2026 edition

The study comprises an analytical panel of 50 units, Codebook v1.0 frozen before final adjudication, and 500 entity-dimension decisions. Eligible public evidence does not meet the predefined coverage thresholds required to support an ordinal classification among units; accordingly, the report presents evidence profiles rather than a comparative hierarchy.

The study estimates only the observable degree of post-quantum transition from public, attributable, and traceable evidence. It does not infer undisclosed internal states, does not impute maturity from documentary silence, and does not make judgments about the overall cybersecurity quality of the units analyzed. The unit of analysis is an organization or operational component with an identifiable Mexican attribution scope; the unit of coding is an entity-dimension claim linked to explicit evidence and scope.

CLOSE OF THE FACTUAL REVIEW PERIOD

All 50 units were included in the formal factual review process. At the close of the period, no response provided a material correction or an eligible public source that changed an adjudication.

Authorship

Author: Dr. Juan Pablo Ybarra Llamas
Publishing entity: Zero Trust Consulting / ZTC Research
Website: https://zerotrust.consulting
Main evidence cutoff: September 2, 2026
Factual review cutoff: September 18, 2026

Recommended citation: Ybarra Llamas, J. P. (2026). *Mexico and the Post-Quantum Transition 2026: Public evidence, attribution, and observable post-quantum maturity.* ZTC Research / Zero Trust Consulting.

ANALYTICAL INDEPENDENCE

To safeguard analytical independence, ZEROPAN Core —a post-quantum cryptographic vault (PQC) with tokenization capabilities, developed by Zero Trust Consulting— was kept outside the analytical panel and the international comparison. Evidence associated with the platform was not part of the corpus used for coding, adjudication, or conclusions.

CONTENTS

Index

Introduction

The transition to post-quantum cryptography (PQC) poses, before a classification problem, a measurement problem under conditions of asymmetric public observability. An organization may perform substantial internal work without disclosing it; conversely, a global statement, a provider capability, or a promotional reference may suggest a degree of progress that cannot be attributed to the Mexican perimeter under analysis.

The research question is deliberately bounded, reproducible, and open to empirical refutation: what degree of post-quantum transition can be supported, as of September 2, 2026, for each Mexican analytical unit exclusively from public, attributable, auditable, and dimensionally sufficient evidence? The estimand is not latent internal preparedness —unobservable under this design— but the post-quantum maturity that can be demonstrated under a prespecified evidence protocol.

> **RESEARCH QUESTION**
>
> What degree of post-quantum transition can be publicly demonstrated, with local attribution and sufficient dimensional evidence, for each unit in the panel as of the cutoff date?

This distinction governs panel selection, the treatment of unobserved data, attribution rules, the separation between coverage and maturity, and the decision not to publish an ordinal classification when evidence does not satisfy comparability thresholds. The report should therefore be interpreted as a study of observability and transition evidence; not as an audit of internal controls, a comprehensive cybersecurity rating, or a population estimate of the Mexican market.

00 /

Executive findings

What can be responsibly stated about the observable post-quantum transition in the analytical panel.

Executive findings

The central result does not support an inference of generalized lag. It supports a narrower and methodologically defensible conclusion: eligible public evidence on organizational post-quantum transition in the analytical panel does not yet achieve the coverage required for a responsible ordinal comparison among panel units.

Under the protocol applied to the analytical panel of 50 units, no unit reached the minimum coverage required to publish an aggregate observable-maturity score (Observable Readiness Score, ORS).

50 analytical units	**500** entity-dimension decisions	**4** estimable dimensional decisions
0 complete ORS	**0** partial ORS	**50** evidence profiles

METHODOLOGICAL INTERPRETATION

A dimension remaining NE does not mean M0, lack of preparedness, or lack of internal work. It means the protocol did not identify sufficient public evidence, with the required locus and attribution, to estimate it. The design preserves the unobserved datum as unobserved; it does not convert it into a negative rating.

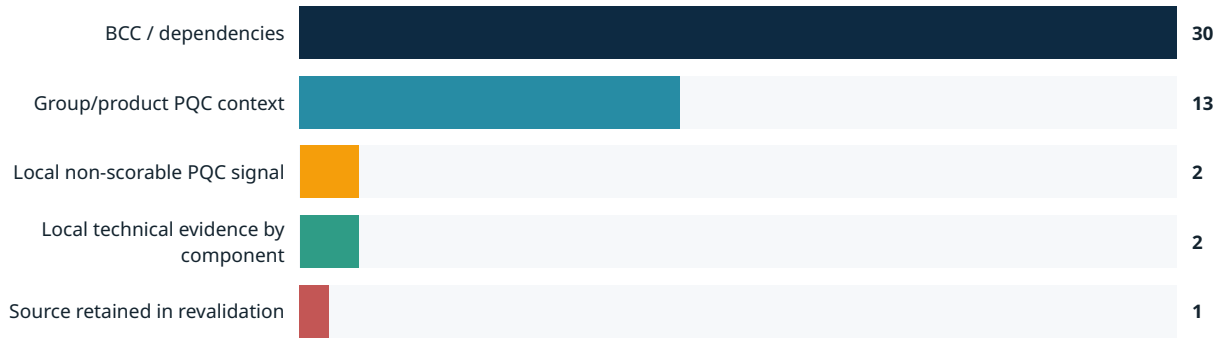

Figure 1. Central pattern of the panel. Counts are non-exclusive. BCC describes publicly observable conventional cryptographic dependencies; it is not equivalent to PQC evidence.

Five principal findings

- Cryptographic dependencies relevant to an eventual transition are considerably more observable than the post-quantum transition itself. Conventional cryptographic dependencies —HSM, KMS, PKI, TLS, encryption, tokenization, or equivalent controls— were identified in 30 of 50 units, while locally estimable PQC evidence appears in only four entity-dimension decisions.
- Cloud infrastructure is the only sector in the panel in which operational post-quantum technical capability could be identified and locally attributed to concrete components in Mexico. AWS Mexico Central and Google Cloud Querétaro reach M4 only in D5 and D8, with EC of 20%. This result describes two estimable dimensions per unit; it does not authorize an inference of organizational maturity equivalent to 80%.
- Global evidence is not automatically attributed to a Mexican operation. Thirteen units present PQC context at group or product level, but the Codebook requires an explicit attribution link when the claim is intended to describe a unit with a Mexican locus.
- Local signals were identified; however, a signal is not equivalent to demonstrated maturity. Santander México and Banorte present local PQC signals; neither, by itself, satisfies the evidence gate required to adjudicate an organizational dimension.
- The international comparison shows public institutionalization through heterogeneous mechanisms: executive orders, roadmaps, guidance, funded pilots, infrastructure, and standardization. The Mexican corpus includes evidence of academic and R&D capacity in PQC, but no national transition instrument comparable to the more structured frameworks in the international corpus was identified at the cutoff.

STUDY THESIS

Cryptographic dependencies relevant to an eventual transition are widely observable; local organizational post-quantum transition, by contrast, still does not reach sufficient coverage for an organizational estimate from public evidence.

01 /

Technical foundation and migration problem

The post-quantum transition extends beyond algorithm substitution: it requires transforming dependencies, trust models, interoperability, and cryptographic lifecycles.

From algorithm standardization to operational migration

Algorithm standardization reduces one source of uncertainty, but shifts the primary challenge toward migrating real architectures, preserving interoperability, and maintaining the continuity of the trust mechanisms that sustain them.

On August 13, 2024, the first three Federal Information Processing Standards (FIPS) resulting from NIST's post-quantum standardization process were published: FIPS 203 (ML-KEM) as a key-encapsulation mechanism, and FIPS 204 (ML-DSA) and FIPS 205 (SLH-DSA) for digital signatures. Standardization reduces algorithmic uncertainty, but by itself does not solve inventory, interoperability, lifecycle management, third-party dependencies, or retirement of legacy components.

The effective unit of migration

Dependency	What changes	Why algorithm enablement is not sufficient
Keys / KMS / HSM	Algorithms, sizes, APIs, rotation	Provider capability does not demonstrate adoption or end-to-end compatibility.
Certificates / PKI	Formats, chains, signatures, and trust stores	Interoperability and renewal can dominate the schedule.
TLS / VPN / SSH	Cryptographic negotiation, hybrid groups, and libraries	Clients, proxies, specialized devices, and protocol intermediaries must interoperate without degradation.
Code and artifacts	Software signing, repositories, and supply chain	Changing signing mechanisms affects validators, HSMs, CI/CD chains, and legacy devices.
Long-lived data	Priority by confidentiality horizon	Risk can accumulate before there is practical capability to compromise public-key cryptography.
Third parties	Roadmaps, contracts, and dependencies	The organization may govern a risk that technically resides with a provider.

Harvest Now, Decrypt Later: a relationship between exposure and migration horizons

Harvest Now, Decrypt Later (HNDL) risk —capturing encrypted information today with the expectation of decrypting it in the future— requires early attention when the sum of the information's required confidentiality lifetime and the time needed to migrate is comparable to, or exceeds, the horizon of a relevant cryptanalytic threat. Because that horizon is uncertain, the study does not assign a materialization date: it uses data longevity and migration time as prioritization variables, not as a prediction of a break date.

> **INTERPRETATION CRITERION**
>
> PQC adoption does not replace existing cryptographic and security controls. Segmentation, key management, rotation, least privilege, resilience, and third-party control remain relevant during and after the transition.

02 /

Methodology: design, panel selection, and estimation

The study separates observable maturity, confidence, and coverage; lack of evidence is treated as unobserved data, not as a zero value.

Methodological design and Codebook v1.0

The central construct is observable post-quantum transition supported by public, attributable, and auditable evidence. The design does not attempt to estimate undisclosed internal states; it seeks to establish which claims can be reproducibly supported for each unit, dimension, and scope.

Research design and estimand

The study adopts an observational, cross-sectional, open-source design with an explicit cutoff date. The estimand is a documentarily observable property: the maturity of PQC transition that can be attributed to a Mexican unit under eligible evidence. This property should not be confused with actual internal maturity, which may be higher, lower, or simply unobservable from the public record.

The unit of analysis is an organization or operational component with a distinguishable Mexican identity and locus; locus means the territorial, organizational, or service scope to which a claim can validly be attributed. For that reason, the report uses “analytical unit” rather than “company” as a general category: the panel includes both organizations and technically separable regional components. The unit of coding is an entity-dimension claim linked to one or more sources and accompanied, at minimum, by scope locus, dependency mode, evidence class, source status, confidence, and adjudication rationale. Inference is restricted to the scope those variables can support.

> **INFERENTIAL SCOPE**
>
> The panel has analytical, not statistical, external validity. Results allow patterns within the selected corpus to be described and observability mechanisms to be contrasted; they do not estimate prevalence for the Mexican market as a whole or assign selection probabilities to organizations in the country.

Selection of the 50-unit analytical panel

The panel is a purposive maximum-variation sample (Patton, 2015), designed to cover heterogeneous configurations of trust, cryptographic dependency, data longevity, and institutional regime. The size n=50 sets an analytical boundary that allows 500 entity-dimension decisions to be reviewed with depth and structural diversity. Selection prioritized structural variation, interorganizational centrality, and diversity of observability regimes within the defined strata. The design is non-probabilistic and does not estimate population parameters.

The final perimeter of 50 units was fixed before final adjudication. Inclusion was independent of the presence, quality, or absence of PQC evidence.

Panel-construction procedure

Stage	Selection rule	Methodological function
1. Functional stratification	Define, before final adjudication, the eight analytical strata and the cryptographic surfaces that had to be represented.	Prevents selection from depending on public notoriety or later PQC results.

Stage	Selection rule	Methodological function
2. Candidate eligibility	Identify units with a Mexican nexus, cryptographic materiality, and sufficient separability to apply attribution rules.	Reduces ambiguity about which entity or component constitutes the unit of analysis.
3. Purposive selection	Prioritize structural variation, interorganizational centrality, and diversity of observability regimes within the strata.	Expands the range of configurations over which the instrument is tested.
4. Freezing	Fix the perimeter before final adjudication and keep inclusion independent of observed PQC evidence.	Limits ex post selection and analytical degrees of freedom.
5. Amendment control	Document any panel modification separately without altering the construct, weights, gates, or thresholds.	Preserves traceability across versions and internal comparability.

Inclusion criterion	Operationalization	Methodological risk controlled
Identifiable Mexican nexus	Mexican entity or operational component with a distinguishable territorial, regulatory, or service locus.	Prevents attribution to Mexico of purely global evidence.
Cryptographic materiality	Control of or dependency on identities, payments, PKI/KMS/HSM, encrypted channels, signatures, long-lived data, or other trust functions.	Avoids units without a substantive relationship to the construct.
Interorganizational centrality	Participation in trust chains, infrastructure, processing, cloud, telecommunications, identity, or public services.	Captures dependencies that extend beyond a single organization.
Sector variation	Deliberate coverage of banking, payments/fintech, telecommunications, cloud/data, insurance, energy/critical infrastructure, health, and digital government.	Reduces excessive concentration in a single disclosure regime.
Analytical separability	The unit must be reasonably distinguishable from its group, product, or provider for attribution analysis.	Reduces double counting and locus ambiguity.
Independence from outcome	The existence of positive, negative, or absent PQC evidence does not determine inclusion.	Avoids selection conditioned on the dependent variable.

Sector composition and analytical function

The sector distribution does not replicate market shares. It is used to cover heterogeneous cryptographic surfaces and different observability regimes, so the instrument can test its attribution and evidence rules in contexts comparable only within its own scope.

Analytical stratum	n	Analytical rationale
Banking and monetary authority	9	Transactions, HSM/PKI, identity, continuity, and group-local structures.
Payments and fintech	12	Tokenization, APIs, payment networks, and interorganizational dependencies.
Telecommunications	6	Identity, network trust, and infrastructure with long lifecycles.
Cloud / data	5	KMS/HSM/TLS, local regions, and dependency on provider capabilities.
Insurance	5	Long-lived personal/financial data and complex corporate structures.
Energy / critical infrastructure	5	IT/OT convergence, certificates, firmware, availability, and roots of trust.
Health	4	Sensitive long-retention data, identity, and institutional infrastructure.

Analytical stratum	n	Analytical rationale
Digital government	4	Population identity, tax/customs, and public services with long-term trust.

RATIONALE FOR PANEL COMPOSITION

The 50 units were selected to maximize structural variation within the eight defined strata. Exclusion of other entities reflected functional redundancy, absence of a separable Mexican locus, or sector concentration. Separate units within the same group were retained only where a distinguishable operational or regulatory perimeter existed. For cloud providers, an identifiable Mexican region defines the component evaluated.

Source identification, screening, and versioning protocol

Collection was conducted by unit and dimension, prioritizing institutional and technical primary sources. Secondary sources were used as discovery or contextual mechanisms, not as automatic substitutes for primary evidence when a claim required technical traceability or local attribution. Each finding was assessed against a specific claim, an applicability scope, and a cutoff date; the mere appearance of PQC terminology was not sufficient for eligibility.

Phase	Operational rule	Control function
1. Discovery	Search by unit, dimension, and cryptographic surface across official domains, technical documentation, regulation, repositories, releases, and institutional materials.	Maximize sensitivity without converting isolated mentions into eligible evidence.
2. Screening	Require relevance to the dimension, source identifiability, validity at cutoff, and attributable scope.	Exclude semantic noise, duplicates, and out-of-scope evidence.
3. Hierarchization	Prioritize primary and technical sources; treat secondary sources as auxiliary signals unless sufficiently corroborated.	Reduce dependence on mediated interpretation and promotional language.
4. Versioning	Record source status and retain changes or disappearances detected during revalidation.	Make documentary drift visible and avoid silent substitution.
5. Close	Close the search by cutoff date and protocol completeness, not by presumed saturation of the web universe.	Avoid presenting the corpus as exhaustive or statistically complete.

OPERATIONAL DEFINITION OF THE ESTIMAND

For each unit i and dimension d, the estimand is the highest M1-M5 level that can be supported with eligible public evidence at the cutoff, after applying attribution and scope rules. If the eligibility gate is not passed, the state remains undefined for maturity purposes (NE), rather than being set to zero. EC_i expresses the share of the ten dimensions that are estimable; any ORS aggregation is subordinate to the frozen reportability thresholds.

Inference model and treatment of unobserved data

Estimation proceeds in three sequential stages. First, the protocol determines whether evidence is eligible for the defined claim and scope; only then can an M1-M5 level be adjudicated. Finally, the coverage of estimable dimensions determines which reporting mode is permissible. This ordering prevents technically strong but misattributed evidence from producing an unsupported local adjudication.

Stage	Methodological question	Output
1. Eligibility	Is the source public, attributable, current, and sufficient for the defined dimension and locus?	Estimable / NE
2. Conditional maturity	If estimable, which M1-M5 level does the evidence demonstrate without exceeding its class and scope?	M1-M5 by dimension
3. Reportability	Does EC coverage permit aggregation and reporting of an ORS under the frozen thresholds?	Profile / partial ORS / complete ORS

Absence of public evidence is not assumed to be random. Propensity to disclose may vary by sector, regulatory regime, business model, operational sensitivity, and documentary practice. Accordingly, the study does not adopt the statistical assumption that data are missing at random (Little & Rubin, 2019), does not impute values, and does not construct sector maturity averages from NE cells. EC measures eligible documentary coverage; not internal performance.

UNOBSERVED-DATA RULE

NE is an epistemic state, not a maturity level. Converting NE into M0 would produce a classification dominated by disclosure practices rather than by evidence of post-quantum transition.

Dimensions and weighting

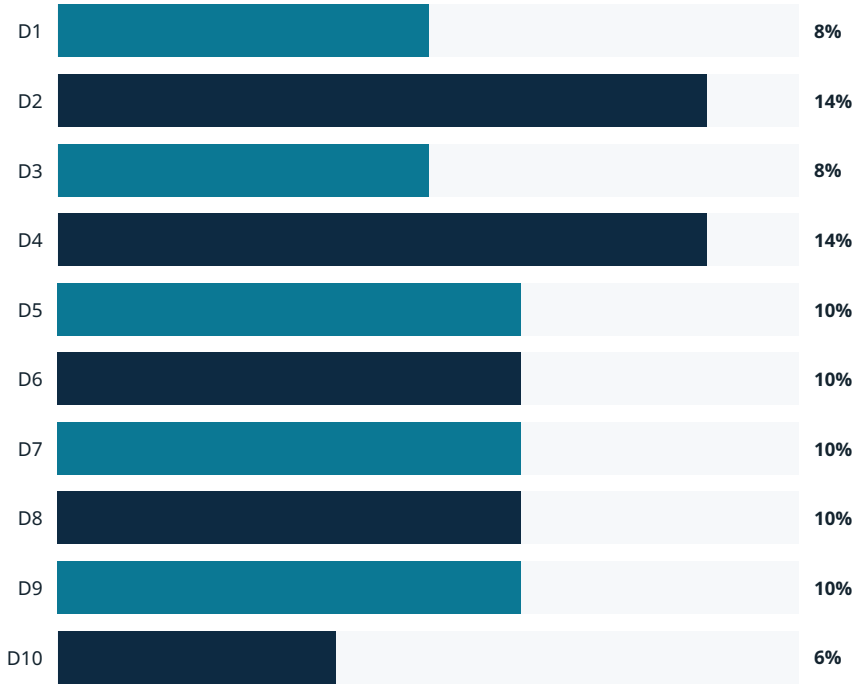

Figure 2. Observable Readiness Score (ORS) weighting. D2 and D4 carry 14%; D10, 6%; the remainder ranges from 8% to 10%.

ID	Dimension	Weight	Gate
D1	Governance and accountability	8%	No
D2	Cryptographic inventory and dependency discovery	14%	Yes
D3	Data longevity and quantum-risk prioritization	8%	No
D4	Crypto-agility and target architecture	14%	Yes
D5	Key, certificate, and trust infrastructure	10%	No
D6	PQC standards and migration design	10%	Yes

ID	Dimension	Weight	Gate
D7	Testing, interoperability, and performance	10%	No
D8	Deployment and transition of legacy components	10%	Yes
D9	Third-party and supply-chain transition	10%	Yes
D10	Migration assurance and resilience	6%	No

Three methodologically independent variables

ORS - OBSERVABLE READINESS SCORE

Weighted maturity only over dimensions that are estimable and reportable. It is not calculated when coverage is insufficient.

EC - EVIDENCE COVERAGE

Percentage of dimensions for which a unit can be estimated under the protocol. It determines which reporting mode may be used.

ECS - EVIDENCE CONFIDENCE SCORE

Quality and traceability of eligible evidence. It informs confidence in an adjudication but is not multiplied by the ORS.

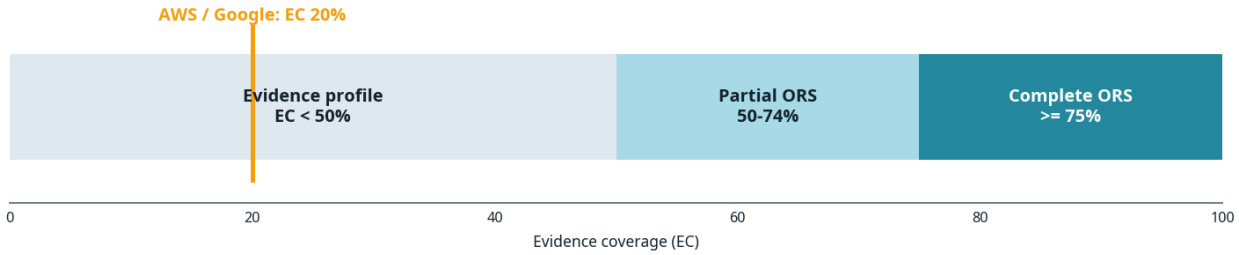

Figure 3. Coverage is a publication gate, not a maturity multiplier. AWS and Google remain evidence profiles with EC=20%.

Measurement properties and reportability thresholds

The M1-M5 levels constitute an operational ordinal scale: they express increasing states of evidence and observable maturity, but the design does not assume constant distance between adjacent categories. The ORS is therefore a composite index defined by the Codebook, not a psychometric interval scale or a direct estimate of a latent variable. Any numerical translation of ordinal categories within the ORS should be read as a transparent scoring convention; if future editions achieve sufficient coverage to aggregate results, that aggregation should be accompanied by sensitivity analysis against alternative monotonic mappings.

The EC thresholds of 50% and 75% are prespecified aggregation and reportability rules, not “natural” cutoffs inferred from the data. Likewise, dimensional weights are design conventions frozen in v1.0, not empirically estimated coefficients. Because no unit exceeds EC=20%, neither the weights nor marginal variations in the thresholds alter the principal inferential result.

NE, BCC, and S/F/T evidence

NE means “not estimable with sufficient public evidence for the defined claim and scope.” If a dimension is NE, maturity remains unestimated and is never transformed into M0. The BCC label separately preserves observable conventional cryptographic dependencies —HSM, KMS, PKI, TLS, tokenization, encryption, or equivalents— without converting them into evidence of PQC transition.

Class	What it demonstrates	Typical ceiling
S · Signal	Recognition of risk, vacancy, executive statement, or promotional signal without demonstrated formal control.	M1
F · Formal	Roadmap, policy, mandate, program, procurement, or contractual requirement.	M2, absent additional evidence
T · Technical	Test, implementation, inventory, repository, protocol, API, or verifiable technical documentation.	Up to M5

Local attribution and applicability

The intrinsic quality of a source does not guarantee that it answers the local question. The Codebook distinguishes MX-DIRECT, MX-COMPONENT, GROUP-GLOBAL, PRODUCT-GLOBAL, JURISDICTION, and UNKNOWN. To attribute a group capability to a Mexican unit, an explicit link is required: Mexico coverage, a shared platform with demonstrated applicability, an identified deployment, a mandatory group policy applicable to the subsidiary, or corroborating local evidence.

- Global evidence is not automatically attributed to Mexico. Corporate affiliation or use of a common provider does not, by itself, constitute an attribution link.
- Provider capability does not constitute evidence of client maturity. Use, control, and scope must be demonstrated.
- A pilot or proof of concept may demonstrate testing activity, but not production deployment unless an explicit and verifiable production perimeter exists.
- Declarative vocabulary —for example, “implemented”, “deployed”, or “quantum-safe”— does not establish M4/M5 by itself; sufficient operational evidence is required.

Reliability, independent coding, and freezing

The process included rounds of independent coding without prior cross-consultation, focused revalidations, and documented adjudication of discrepancies. Reliability claims are limited to the subsets that were actually double-coded (Krippendorff, 2018). Codebook v1.0 was frozen and version-controlled before adjudication closed.

> **FREEZE RULE AND CONTROL OF ANALYTICAL DEGREES OF FREEDOM**
>
> During the factual review process, a newly identified public source could reopen only the affected dimension if it was eligible under the main cutoff. Weights, methodological gates, thresholds, inheritance rules, and the Codebook remained frozen. This control limits analytical degrees of freedom and reduces ex post adjustments oriented by the results.

Robustness test of the reportability threshold

The maximum observed coverage is EC=20%. Consequently, no unit has a reportable organizational ORS under any threshold strictly above 20%; the result remains far from the 50% and 75% gates. Sensitivity analysis shows that the principal conclusion does not depend on a marginal choice of threshold and does not justify relaxing the Codebook.

M1-M5 maturity scale

Level	Reading	Evidence burden
M1	Recognized risk or need	Recognition or intent with explicit PQC linkage.
M2	Formal direction defined	Responsible owner, method, design, roadmap, or formal requirement.
M3	Verifiable execution	Completed inventory, performed test, or controlled pilot with result.
M4	Controlled operation	Production or repeatable process with lifecycle, monitoring, controlled rollback, or governed decisions.
M5	Continuous integration	Capability embedded in the engineering/risk cycle with measurement, evolution, and retirement of legacy components.

M4 and M5 require substantially stronger operational evidence. Verbs such as “implemented”, “deployed”, or “quantum-safe” are not sufficient, by themselves, to establish those levels.

03 /

International comparison and Mexico context

The international comparison does not rank countries: it contrasts types of public instruments, authority, scope, milestones, and execution signals.

International comparison and Mexico context

The international comparison is interpretable only when the nature of each instrument is distinguished. An executive order, a government roadmap, technical guidance, a funded pilot program, or a provider capability represent different forms of institutionalization and execution and should not be treated as equivalent units.

Jurisdiction	Public instrument	Scope	Methodological reading
United States	Executive Order 14412, Jun 22, 2026	Federal systems, procurement, and support for critical infrastructure	Ordered federal milestones; procurement requirements and accelerated validation.
Canada	Cyber Centre - Government of Canada roadmap	Federal departments/agencies	Initial plan Apr-2026; high priority 2031; remainder 2035.
United Kingdom	NCSC - PQC migration timeline	Public and private organizations; national guidance	Discovery and initial plan by 2028; high priority by 2031; migration by 2035.
European Union	Coordinated Implementation Roadmap	Member states, public sector, and critical infrastructure	Coordinated roadmap; milestones and coexistence / crypto-agility approach.
Singapore	Quantum-Safe Migration Handbook + QRI	CII, government, and organizations	Operational guide + self-assessment instrument published Jul-2026.
Australia	ASD planning for PQC	Public and private organizations	Plan 2026; begin critical systems 2028; complete 2030.
Japan	Cybersecurity Strategy 2025	Government; extension to critical infrastructure and private sector	Government targets 2035; roadmap for FY2026.
South Korea	KISA - 2026 transition pilot program	Telecom, finance, transport, defense, and space	Funded pilots for transition and infrastructure validation.
Brazil	Portaria ITI No. 38/2026 · GTT-PQC/ICP-Brasil	ICP-Brasil and digital-trust ecosystem	Formal technical group; diagnosis, migration plan, regulatory update, and execution strategy.
Mexico	Public R&D and academic capacity; no comparable national instrument identified at cutoff	Academic research; reviewed federal public record	IPN/INAOE provide evidence of PQC R&D; no equivalent national transition instrument was identified at cutoff.

Valid conclusions from the international comparison

Public institutionalization of the transition is already occurring through heterogeneous instruments. One country may adopt an executive order; another, a technical roadmap; another, funded pilots; another, a guide accompanied by a self-assessment tool. These instruments differ in authority, scope, binding force, and degree of execution; the study uses them as comparators of institutional architecture, not as a national security ranking.

Mexico: PQC R&D, without a comparable national transition instrument identified at cutoff

The reviewed Mexican public record documents academic and R&D activity: CIC-IPN reports in 2026 a project to develop post-quantum public-key infrastructure (PKI) for IPN applications, and INAOE maintains PQC among its research lines. At the cutoff, the protocol did not identify in the reviewed public record a national post-quantum transition program at federal or sector level.

04 /

Consolidated results

All 50 units remain evidence profiles. Only two units present locally estimable technical evidence, and only in two dimensions each.

Consolidated results

0 / 50	0 / 50	50 / 50
complete ORS · EC 75-100%	partial ORS · EC 50-74%	evidence profile · EC <50%

Only AWS Mexico Central and Google Cloud Querétaro present locally estimable dimensions, each with two of ten dimensions. No unit reaches an EC of at least 50%; therefore, the protocol does not permit publication of a partial or complete ORS.

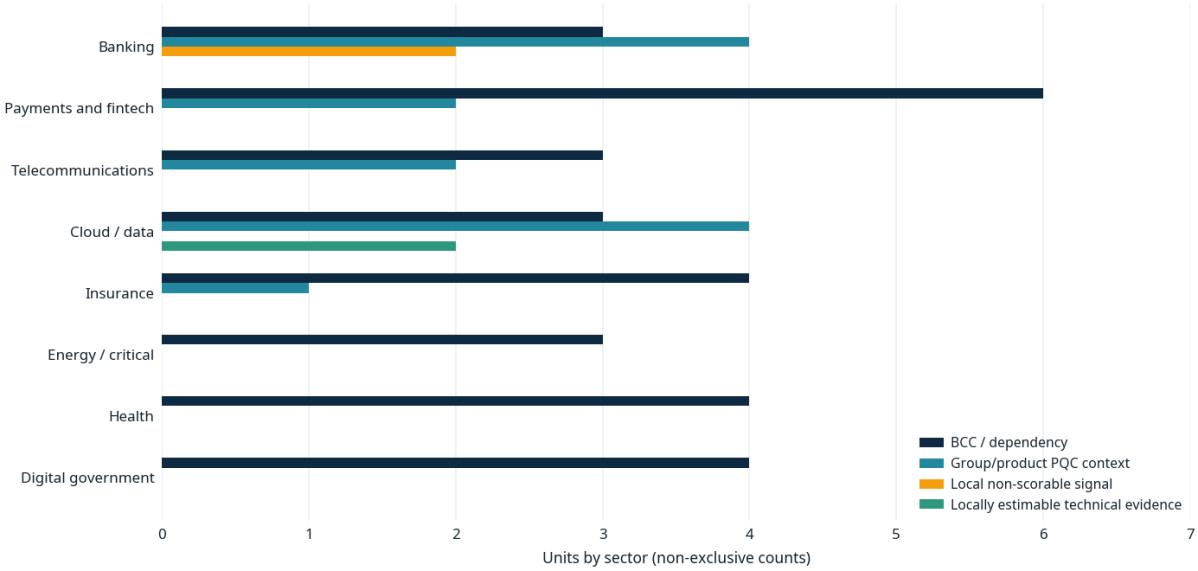

Figure 4. Observability by sector within the panel. Counts are non-exclusive and do not constitute population rates.

Cloud infrastructure: the only area with locally estimable technical evidence

Unit	Estimable dimensions	EC	Scope	Reportable result
AWS Mexico Central	D5 = M4; D8 = M4	20%	MX-COMPONENT / DIRECT	Evidence profile
Google Cloud Querétaro	D5 = M4; D8 = M4	20%	MX-COMPONENT / DIRECT	Evidence profile

AWS KMS documents hybrid ML-KEM in TLS for non-FIPS endpoints across all regions in the aws partition; the AWS Mexico (Central) Region, mx-central-1, has operated since January 14, 2025. Google Cloud documents general availability of ML-DSA, SLH-DSA, and ML-KEM in Cloud KMS; the service is available in northamerica-south1 (Mexico), whose infrastructure zones are located in Querétaro. Under the Codebook, this combination supports attribution of capability to concrete local components; it does not support inference of complete organizational maturity or customer adoption.

RESTRICTION ON INTERPRETATION OF M4

M4 describes the maturity of an estimable dimension, not of the organization as a whole. With EC=20%, the Codebook prohibits producing an aggregate ORS. “Two dimensions at M4” and “80% organizational maturity” are methodologically different claims; only the former is supported.

Santander México and Banorte: local signals without sufficient evidence for a maturity adjudication

Santander México presents a public local signal related to PQC, but Santander Group initiatives are not attributed to Mexico without an explicit link. Banorte presents a local signal that does not pass the evidence gate required to adjudicate maturity.

Reading the result of 500 dimensional decisions

Of the 500 entity-dimension decisions, four were estimable. The remaining 496 did not pass the evidence gate for the defined claim, scope, and dimension. The methodology preserves those decisions as non-estimable and avoids imputing values where the public record does not allow observation.

ROBUSTNESS OF THE PRINCIPAL RESULT

The maximum observed EC is 20%. Consequently, the conclusion “0 reportable organizational ORS” holds for any reportability threshold above 20%. The distance from 50% and 75% indicates that the result does not depend on a marginal variation in the frozen thresholds.

Executive implications

- This edition does not publish an ordinal classification among units. Constructing one with insufficient coverage would introduce apparent precision not supported by the evidence.
- The absence of an aggregate score is a methodological result: it identifies where locally attributable and dimensionally sufficient evidence is missing.
- In future editions, the instrument is designed to detect early variation in inventory, local attribution links, testing, and third-party governance before requiring evidence of large-scale deployments.

INFERENTIAL SCOPE

With a maximum EC of 20%, none of the 50 units reaches the coverage required for an organizational ORS. The reportable result is therefore an evidence profile.

05 /

Sector reading

Observability varies by sector. Documentation, architecture, outsourcing, and asset lifecycles condition what can be demonstrated publicly.

Sector reading

Sector	n	Ctx	BCC	Signal	Tech.	Retained source	Reading
Banking and monetary authority	9	4	3	2	0	1	The principal constraint on estimability is the absence of public attribution links between group programs and Mexican systems.
Payments and fintech	12	2	6	0	0	0	Visible cryptographic dependencies; rarely connected publicly to a local PQC strategy.
Telecom	6	2	3	0	0	0	Global context and BCC exist, but local evidence is fragmented.
Cloud / data	5	4	3	0	2	0	Only sector with locally estimable technical evidence; greater documentary observability, not necessarily greater internal maturity.
Insurance	5	1	4	0	0	0	Long-lived data and observable BCC; little local organizational PQC evidence.
Energy / critical	5	0	3	0	0	0	Criticality does not authorize inference of transition; insufficient local evidence for estimation.
Health	4	0	4	0	0	0	BCC across the entire subpanel; longevity is relevant to HNDL, without presuming migration.
Digital government	4	0	4	0	0	0	Visible conventional dependencies; no locally estimable PQC transition identified.

Observability is conditioned by the disclosure regime

Cloud providers publish technical documentation, APIs, regions, algorithms, and roadmaps at a level of detail that allows locus and capability to be closed at component level. Banks, insurers, health institutions, or critical infrastructure operators may conduct substantial internal work while disclosing very little. This missing-data mechanism is plausibly non-random; therefore, sector differences in observability are not interpreted as a hierarchy of security or maturity. Sector counts describe the public record of the panel, not the prevalence of internal preparedness; comparing sectors as though they shared the same propensity to disclose would produce an inference the design does not support.

06 /

Payments: interorganizational cryptographic dependency

In payments, the post-quantum transition does not end with ML-KEM: it involves keys, signatures, certificates, PAN, tokenization, APIs, processors, networks, and third parties within an interoperable architecture.

The transition as an interorganizational chain of trust

The cryptographic surface subject to migration crosses organizational boundaries; therefore, provider governance is a structural component of the transition.

Payment systems combine components that rarely change at the same pace: HSM, PIN/EMV, TLS, PKI, tokenization, network keys, APIs, terminal software, processors, and third-party agreements. Post-quantum migration can fail even when algorithm selection is correct if one link cannot negotiate, rotate, validate, or be retired in a coordinated way. In this context, PAN refers to the Primary Account Number.

Five structural sources of complexity in payments

#	Challenge	Implication
1	Distributed inventory	Cryptographic dependencies reside in applications, HSMs, certificates, networks, providers, and contracts.
2	Compatibility	Classical/PQC coexistence may last for years; stronger cryptographic negotiation loses utility if one component prevents interoperability.
3	Asymmetric lifecycles	Cards, terminals, specialized devices, software, and cloud services renew at different rates.
4	Custody and responsibility	An organization may be responsible for managing a risk whose technical dependency resides with a third party.
5	Assurance	Migrating without controlled rollback, regression testing, monitoring, and retirement of legacy components can introduce additional risk.

ARCHITECTURE QUESTION

Which cryptographic dependency does the organization actually control, which is controlled by a third party, and what contractual or technical evidence exists that both will migrate in the correct order?

07 /

Prioritization by exposure horizon

Risk prioritization does not depend on predicting when a cryptographically relevant quantum computer will become available; it depends on relating longevity, migration time, and exposure.

Prioritization by exposure horizon

The prioritization problem can be formulated precisely: for how long must this asset remain confidential or authentic, how long will migration take, and what dependencies prevent that change? This decision framework separates material urgency from generic risk formulations.

Asset	Horizon	Transition question
Identity / population	Long	Must biometrics or identity evidence remain protected beyond the current renewal cycle?
Health	Long	Which records or sensitive data retain value for decades?
Finance / payments	Variable	Which data, signatures, or credentials outlive the system that protects them today?
Critical infrastructure	Long / operational	Which secrets, firmware, certificates, or channels have extended lifecycles?
Ephemeral sessions	Short	Is the real priority cryptographic negotiation, availability, and compatibility rather than long-term confidentiality?

The study does not assign HNDL probabilities to specific organizations from public evidence. It uses longevity as a prioritization dimension and as a reminder that cryptographic exposure can accumulate before technological change becomes externally visible.

08 /

From cryptographic inventory to operational resilience

In the 2027 cycle, the evidence with the greatest analytical value will be evidence that connects inventory, prioritization, design, testing, deployment, retirement, and assurance.

From cryptographic inventory to operational resilience

Under this design, the post-quantum transition becomes observable first as a discipline of architecture, inventory, and dependency management; subsequently, as controlled deployment and retirement.

Stage	Evidence that increases estimability
1. Discover	Cryptographic inventory linked to assets, owners, data, and third parties.
2. Prioritize	Data longevity, criticality, dependency, and renewal horizon.
3. Design	Target architecture, crypto-agility, standards, and hybrid/coexistence strategy.
4. Test	Interoperability, performance, failure modes, controlled rollback, and reproducible evidence.
5. Deploy	Production within a defined scope with observability and exception management.
6. Retire	Retire vulnerable algorithms, roots of trust, and legacy components; demonstrate that no residual paths remain.
7. Assure	Monitor, measure, revalidate providers, and exercise recovery.

Priority evidence for the 2027 cycle

If the public record begins to show inventories, roadmaps, tests, regional capabilities, provider governance, retirement of legacy components, and assurance, the instrument will be able to measure change with greater coverage. The objective is not to maximize the number of scores, but to increase the design's ability to discriminate real differences in evidence without sacrificing construct validity.

What to monitor in the next cycle

- Publication of inventories or cryptographic-discovery methods.
- Roadmaps with accountable owners, scope, and milestones.
- Explicit attribution links between global programs and Mexican operations.
- Regional KMS/HSM/PKI/TLS support and production evidence.
- Pilots with documented results, performance, and interoperability.
- PQC requirements in procurement processes and third-party contracts.
- Retirement of vulnerable algorithms and coexistence controls.
- Metrics, exceptions, controlled rollback, and migration resilience.

09 /

Analytical panel of 50 units / evidence profiles

All units remain evidence profiles; presentation order is sectoral and does not express a maturity hierarchy.

Analytical panel of 50 units

Purposive panel of 50 units. Counts should not be extrapolated as a population estimate for all Mexican organizations.

Banking and monetary authority

Unit	Output	Evidence note
Santander México	Evidence profile	Local PQC signal insufficient for an estimable dimension; group context without sufficient local attribution.
Banorte	Evidence profile	Local signal insufficient to adjudicate maturity.
BBVA México	Evidence profile	Group/product context without a sufficient local attribution link.
Citi México	Evidence profile	Insufficient context for a local ORS.
HSBC México	Evidence profile	Insufficient context for a local ORS.
Scotiabank México	Evidence profile	Insufficient context for a local ORS.
Banco de México	Evidence profile	No locally estimable dimensions under the protocol.
Banamex	Evidence profile	No locally estimable dimensions under the protocol.
Banco Inbursa	Evidence profile	No locally estimable dimensions under the protocol.

Payments and fintech

Unit	Output	Evidence note
Visa México	Evidence profile	No locally estimable dimensions under the protocol.
Mastercard México	Evidence profile	Global context is not equivalent to local maturity.
Prosa	Evidence profile	BCC dependencies do not, by themselves, constitute evidence of PQC transition.
Cecoban	Evidence profile	BCC dependencies do not, by themselves, constitute evidence of PQC transition.
STP	Evidence profile	No locally estimable dimensions under the protocol.
Clip	Evidence profile	No locally estimable dimensions under the protocol.
Conekta	Evidence profile	No locally estimable dimensions under the protocol.
Nu México	Evidence profile	No locally estimable dimensions under the protocol.
E-Global	Evidence profile	No locally estimable dimensions under the protocol.
Mercado Pago Wallet México	Evidence profile	No locally estimable dimensions under the protocol.
Spin by OXXO	Evidence profile	Signal/context insufficient for an estimable dimension under the protocol.
Ualá México	Evidence profile	No locally estimable dimensions under the protocol.

Telecommunications

Unit	Output	Evidence note
AT&T México	Evidence profile	Context/BCC without sufficient attribution link or detail.
Telefónica Movistar México	Evidence profile	Global PQC context without a sufficient Mexican attribution link.
América Móvil México	Evidence profile	Observable BCC/dependencies; no estimable local transition.
Grupo Televisa / izzi	Evidence profile	No locally estimable dimensions under the protocol.
Megacable	Evidence profile	No locally estimable dimensions under the protocol.
Totalplay	Evidence profile	No locally estimable dimensions under the protocol.

Cloud and data infrastructure

Unit	Output	Evidence note
AWS Mexico Central	Evidence profile	D5=M4, D8=M4, EC=20%, MX-COMPONENT / DIRECT.
Google Cloud Querétaro	Evidence profile	D5=M4, D8=M4, EC=20%, MX-COMPONENT / DIRECT.
Microsoft Azure Mexico Central	Evidence profile	Provider context or capability without sufficient local evidence for an ORS.
Oracle Cloud México	Evidence profile	Provider context or capability without sufficient local evidence for an ORS.
KIO Networks	Evidence profile	No locally estimable dimensions under the protocol.

Insurance

Unit	Output	Evidence note
BBVA Seguros México	Evidence profile	Insufficient context for a local ORS.
MetLife México	Evidence profile	BCC/dependencies; no estimable local PQC transition.
Quálitas	Evidence profile	BCC/dependencies; no estimable local PQC transition.
Seguros Banorte	Evidence profile	BCC/dependencies; no estimable local PQC transition.
GNP Seguros	Evidence profile	BCC/dependencies; no estimable local PQC transition.

Energy and critical infrastructure

Unit	Output	Evidence note
CENACE	Evidence profile	Criticality/BCC does not authorize inference of PQC transition.
CENAGAS	Evidence profile	Criticality/BCC does not authorize inference of PQC transition.

Unit	Output	Evidence note
CNE	Evidence profile	No locally estimable dimensions under the protocol.
CFE	Evidence profile	BCC/dependencies; no estimable local PQC transition.
Pemex	Evidence profile	BCC/dependencies; no estimable local PQC transition.

Health

Unit	Output	Evidence note
IMSS	Evidence profile	Observable BCC/dependencies; no estimable local PQC transition.
ISSSTE	Evidence profile	Observable BCC/dependencies; no estimable local PQC transition.
IMSS-Bienestar	Evidence profile	Observable BCC/dependencies; no estimable local PQC transition.
Secretaría de Salud / CCINSHAE	Evidence profile	Observable BCC/dependencies; no estimable local PQC transition.

Digital government

Unit	Output	Evidence note
ATDT	Evidence profile	BCC/dependencies; no estimable local PQC transition.
RENAPO	Evidence profile	BCC/dependencies; formal institutional response: no institutional public source documenting PQC transition was identified; no estimable dimension.
SAT	Evidence profile	BCC/dependencies; no estimable local PQC transition.
ANAM	Evidence profile	BCC/dependencies; no estimable local PQC transition.

10 /

Validity, sources, and traceability

The strength of the result depends on the claims the evidence can support, the inferences the method excludes, and the ability to reconstruct each adjudication.

Validity, observability biases, and inferential limits

- Purposive panel: counts describe the 50 coded units; they are not population estimates and do not support prevalence inferences for all Mexican organizations.
- Temporal validity: sources may change, disappear, or be updated. The main evidence cutoff is September 2, 2026.
- Unobserved data: NE is not M0; a non-estimable dimension remains without a value and does not artificially reduce a score.
- Construct separation: conventional-cryptography evidence is preserved as BCC, but is not transformed into PQC transition without an explicit link.
- Local attribution: group programs, provider capabilities, and global products require separate evidence of applicability when the claim concerns Mexico.
- Factual review: only a factual correction or a new verifiable public source could modify an adjudication; the methodology remained frozen.
- Validation scope: the study evaluates public evidence of PQC transition; internal configurations, control effectiveness, and compliance are outside the estimand.

Threats to validity and design safeguards

Threat	Inference risk	Safeguard
Disclosure bias	Public visibility may differ by sector and institutional regime.	EC separated from maturity; NE is not imputed; no sectoral ordinal classification is published.
Attribution error	Group or provider evidence may be improperly attributed to Mexico.	Explicit locus, inheritance rules, and mandatory attribution link.
Non-random missing data	Documentary silence may correlate with operational sensitivity or disclosure practice.	NE as non-observation; no implicit M0 and no averages with missing cells.
Source drift	Web content may change after coding.	Cutoff date, source status, revalidation, and retention of changed sources.
Researcher degrees of freedom	Ex post changes to weights, gates, or thresholds could favor results.	Frozen Codebook, documented amendments, and separate adjudication.
Temporal validity	PQC transition is dynamic.	Dated results; future replication should apply the same protocol or document a new version.

Methodological references

Patton, M. Q. (2015). *Qualitative Research & Evaluation Methods* (4th ed.). SAGE. Krippendorff, K. (2018). *Content Analysis: An Introduction to Its Methodology* (4th ed.). SAGE. Little, R. J. A., & Rubin, D. B. (2019). *Statistical Analysis with Missing Data* (3rd ed.). Wiley.

Primary references - standards, policy, and migration

National Institute of Standards and Technology (2024). FIPS 203, 204, and 205: Official source

NCCoE / NIST. Migration to Post-Quantum Cryptography: Official source

The White House (2026, June 22). Executive Order 14412 - Securing the Nation Against Advanced Cryptographic Attacks: Official source

Canadian Centre for Cyber Security. Roadmap for the migration to post-quantum cryptography for the Government of Canada: Official source

UK National Cyber Security Centre. Timelines for migration to post-quantum cryptography: Official source

European Commission / NIS Cooperation Group (2025). Coordinated Implementation Roadmap for the Transition to PQC: Official source

Australian Signals Directorate. Planning for post-quantum cryptography: Official source

Cyber Security Agency of Singapore (2026, July 16). Quantum-Safe Migration Handbook and Quantum Readiness Index: Official source

Japan National Cybersecurity Office (2025). Cybersecurity Strategy 2025: Official source

KISA (2026). Post-quantum cryptography pilot transition programme: Official source
Instituto Nacional de Tecnologia da Informação (Brazil). Portaria ITI No. 38 — GTT-PQC/ICP-Brasil: Official source

Primary references - Mexico and cloud infrastructure

CIC-IPN (2026). Development of a post-quantum public-key infrastructure (PKI) for applications at IPN: Official source
INAOE. Research line in post-quantum cryptography: Official source
AWS Key Management Service. Hybrid post-quantum TLS: Official source
AWS (2025, January 14). AWS Mexico (Central) Region, mx-central-1: Official source
Google Cloud (2026, August 11). Post-quantum cryptography roadmap: Official source
Google Cloud KMS (2026, July 28). Quantum-safe digital signatures and ML-KEM: Official source
Google Cloud. Cloud KMS locations / Compute Engine regions and zones — northamerica-south1 (Mexico/Querétaro): Official source

Study traceability

The traceability register preserves the 500 entity-dimension decisions with dimension, weight, estimability, maturity, points, scope locus, dependency mode, S/F/T evidence class, evidence identifiers, source status, ECS, URL, and adjudication rationale. The final perimeter and Codebook v1.0 were kept under version control. The final validity review checked consistency of attribution, scope, causal language, treatment of unobservable evidence, and congruence between the traceability register and the reported conclusions.

> **REPRODUCIBILITY**
>
> Reproducibility depends on each adjudication being reconstructible from the source, scope, applied rule, and rationale. The design prioritizes that traceability over score density.

Minimum replication protocol

Step	Reproducible requirement
1	Fix the Codebook version and cutoff date before adjudication.
2	Collect evidence by unit-dimension and record source, locus, and status.
3	Resolve eligibility before assigning M1-M5; preserve NE without imputation.
4	Apply independent coding/adjudication and document disagreements.
5	Calculate EC and only then determine whether ORS may be published.

— /

Strategic implications

Under this design, the post-quantum transition becomes observable as a discipline of architecture, inventory, and dependency management and, later, as controlled deployment and retirement.

Closing

This first edition does not find sufficient empirical basis to support an ordinal classification among the units in the panel. Its principal contribution is to identify and characterize the gap between the observability of cryptographic dependencies and the observability of a locally attributable post-quantum transition.

That contrast guides the agenda for the next cycle. In 2027, the methodologically most relevant indicator will be whether the gap narrows through evidence of inventories, roadmaps, tests, regional capabilities, third-party governance, retirement, and assurance. If coverage exceeds the predefined thresholds, the ORS will be able to discriminate organizational differences without substituting inference for evidence.

> **CRYPTOGRAPHIC-GOVERNANCE QUESTION**
>
> Which components concentrate critical cryptographic trust functions, and to what extent can the organization identify, govern, replace, and demonstrate its ability to migrate them?

Strategic implications

The strategic issue is not to declare PQC adoption, but to demonstrate which cryptographic dependencies must change, who exercises control over them, which data and trust mechanisms are exposed to extended horizons, and through what migration architecture they can be replaced without degrading security, interoperability, or continuity.

ZERO TRUST CONSULTING
https://zerotrust.consulting