Quantum-Resilient Organizational Identity

Governance, Business Wallets, and PQC Corridors

A governance and systems-architecture analysis for B2B, B2G, G2G, M2M, and agent-to-agent ecosystems

Brian Couzens
SITG Consulting
brian.couzens@sitg-consulting.com

Dr. Carsten Stöcker
CEO, Spherity GmbH
carsten.stoecker@spherity.com

Prof. Dr. Ingrid Vasiliu-Feltes
University of Miami, Herbert Business School
ivfeltes@miami.edu

Authors listed in alphabetical order.

Abstract

Digital identity is becoming a core trust layer for organizational interaction across public administration, enterprise systems, data spaces, machines, and AI agents. Current identity infrastructures still largely depend on elliptic-curve public-key cryptography, long-lived trust anchors, and layered trust chains. Recent resource estimates for ECDLP-256 attacks, together with finalized NIST post-quantum cryptography standards and national migration guidance, support advance migration planning rather than isolated algorithm replacement [1–7]. This article analyzes organizational identity in the quantum transition and distinguishes the confidentiality risk of harvest-now, decrypt-later attacks from the integrity and evidentiary risks created by future forgery of legacy digital signatures. The central risk is therefore not only retrospective disclosure, but a future loss of the public-key trust fabric itself. Quantum-enabled compromise or forgery of issuer, registry, status, revocation, or holder-binding keys could create false organizational authority, manipulated compliance evidence, and even a collapse of critical or digital public infrastructures in domains where authenticity, integrity, and non-repudiation are difficult to restore after the fact.

The article conceptualizes business wallets, including the proposed European Business Wallet, as organizational interfaces for verifiable credentials, secure exchange, and delegated authority [8, 9]. It treats the qualified Verifiable Data Registry, or qVDR, as a functional registry and verification substrate for identifier resolution, credential status, revocation, timestamping, integrity proofs, and audit trails; in European implementations, qVDR-like functions may draw on qualified trust services or qualified electronic ledger infrastructure where applicable legal requirements are met [10, 11]. Verifiable LEIs are treated as bridge mechanisms for cross-jurisdiction legal-entity identification and selected representation rights [12, 13]. The article's main contribution is the PQC Corridor: a bounded governance and technical migration domain in which defined actors coordinate scope, legal and organizational assurance, data and evidence horizons, trust boundaries, cryptographic profiles, and operational controls for high-value organizational identity use cases, while reusable evidence outputs are generated by the corridor.

1 Introduction

Digital identity has become a cross-ecosystem trust layer rather than a narrow administrative function. It enables access to services, market participation, trusted data exchange, and legally

relevant records across public administration, enterprise systems, industrial networks, and cross-border digital processes.

This article examines digital identity in the context of the quantum transition. Quantum computing threatens the cryptographic assumptions that support authentication, signatures, key exchange, and non-repudiation assurances in current identity systems. The impact is amplified by AI-enabled fraud, long software and hardware lifecycles, and dense interdependence across digital ecosystems. In this environment, stolen or compromised identities can affect supply chains, public services, financial systems, and industrial operations.

The analysis focuses on organizational identity. Policy discussions in the digital identity domain often emphasize citizens and consumer authentication, yet legal entities and the actors representing them require dedicated treatment. Identity systems must represent organizational continuity, changes in representation rights, and the validity periods of roles or mandates, including those exercised by software services, devices, and AI agents.

Post-quantum cryptography policy discussions increasingly frame the migration as a critical-infrastructure issue and focus on today's harvest-now, decrypt-later (HNDL) exposure, cryptographic inventories, and phased migration away from quantum-vulnerable algorithms [2–7]. Organizational identity adds a distinct assurance and coordination problem. In regulated industries and critical infrastructure, relying parties need legally meaningful proof of entity existence, representation rights, delegated mandates, issuer authority, credential status, revocation, and evidentiary continuity. These requirements cannot be addressed by algorithm replacement alone. They require cryptographic agility embedded in identity governance so that credentials, signatures, seals, trust anchors, and verification services can remain legally reliable while keys and algorithms change. Figure 1 frames this challenge as a two-dimensional design space. Low assurance and low agility produce weak legacy systems. High agility without assurance creates technical islands with limited legal reliance. High assurance without agility creates brittle compliance and future evidentiary fragility. The target zone is high legal or organizational assurance combined with high cryptographic agility.

This article presents three claims. First, digital identity governance must evolve from periodic compliance control toward continuous resilience governance that can adapt to cryptographic change and ecosystem risk. Second, quantum migration in identity ecosystems cannot be achieved through isolated institutional action because interoperability, trust-anchor rotation, and liability are distributed across multiple actors. Third, organizational identity requires common trust instruments that can operate across jurisdictions. In the near term, verifiable LEIs can provide a basic way to identify legal entities and confirm certain roles in jurisdictions where cross-border mutual recognition remains incomplete. The central contribution is the PQC Corridor, defined here as a bounded environment in which relevant actors align scope, legal and organizational assurance, data and evidence horizons, trust boundaries, cryptographic profiles, and operational controls to address cryptographic agility and the network-effect bottleneck in post-quantum migration.

The remainder of the article is structured as follows. Section 2 analyzes the quantum-era risk landscape for organizational identity. Section 3 reviews the legal and regulatory frameworks that shape identity governance. Section 4 defines the architectural components required for quantum-resilient organizational identity, with emphasis on business wallets, qDPI, and qVDRs. Section 5 formalizes PQC Corridors as the core governance model. Section 6 addresses adoption challenges and implementation pathways. Section 7 sets out the integrated systems architecture required for migration. Section 8 presents strategic implications, and Section 9 concludes.

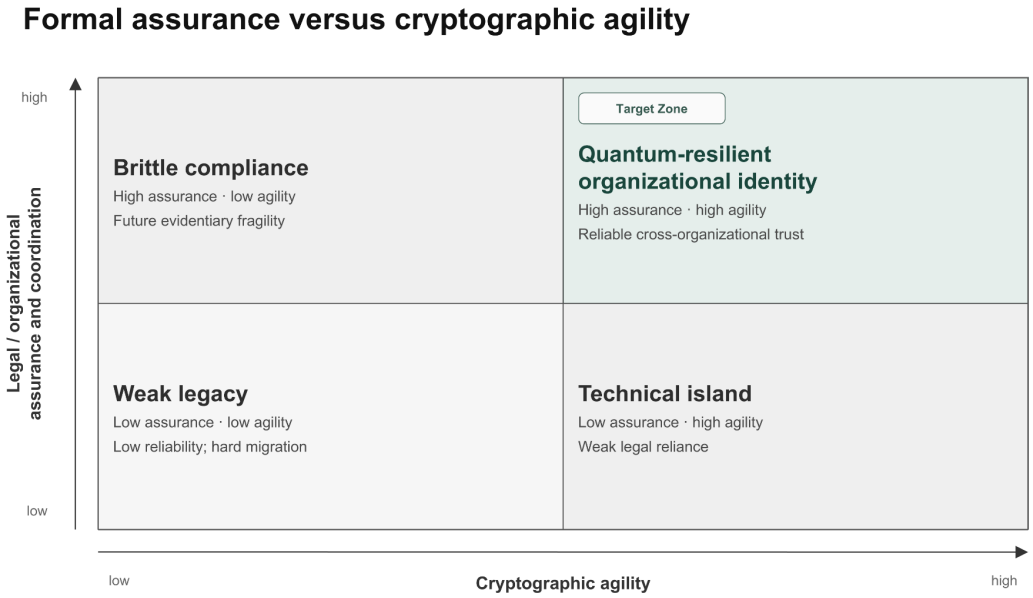

Figure 1: Formal assurance versus cryptographic agility. The matrix distinguishes four states of organizational identity infrastructure according to legal or organizational assurance and cryptographic agility. The target zone is the high-assurance, high-agility quadrant, where identity credentials, trust anchors, verification services, and operational controls can preserve legal reliance while algorithms, keys, and trust-anchor lifecycles change.

2 Quantum-Era Risk Landscape for Organizational Identity

Digital identity in business and public-sector environments depends on interconnected networks. Organizations interact with suppliers, customers, regulators, logistics providers, certification bodies, financial institutions, cloud operators, and software services. In dynamic value chains, these interactions often arise between actors without a prior contractual or technical relationship. Traditional federation models struggle in such settings because they assume predefined trust relationships and a limited number of trust anchors. As ecosystems scale, bilateral onboarding and static integration become costly and slow.

This structural change helps explain the growing relevance of decentralized identity patterns. Decentralized identifiers and verifiable credentials allow issuers, holders, and verifiers to exchange proofs without continuous dependence on a central identity provider [14, 15]. This matters for organizational identity because counterparties often need only limited information, such as whether the organization legally exists, who can represent it, which role a person holds, whether it is certified, or what authority has been delegated. Selective disclosure reduces data exposure, and portable credentials support cross-sector reuse in supply chains, data spaces, and machine-to-machine environments.

Quantum risk affects this ecosystem at several layers. Future cryptographically relevant quantum computers are expected to compromise the public-key algorithms that protect much of today's identity infrastructure. This threatens signatures, certificate chains, key exchange, and the evidentiary value of records that depend on vulnerable cryptography. Recent resource estimates for ECDLP-256 over secp256k1 show that, under particular assumptions, the physical-qubit requirements for some attacks may be lower than earlier estimates [1]. These estimates do not provide an exact timeline, but they strengthen the case for advance migration planning. NIST's

finalized PQC standards and NCSC migration guidance further support the need for structured transition programs [2–5]. Figure 2 summarizes selected standards and regulatory anchors that frame this planning context.

Figure 2: Selected migration anchors for PQC Corridor prioritization. Summary of selected standards and regulatory anchors relevant to corridor planning, including post-quantum cryptography standards, national migration guidance, European roadmap activity, and financial-sector coordination.

Encryption and signing create different migration priorities. Harvest-now, decrypt-later risk makes encryption migration urgent for data with long confidentiality horizons. Adversaries can collect encrypted traffic, credential data, registry records, or supply-chain evidence today and target them for decryption later. This affects product records, compliance documentation, industrial communications, and official regulatory documents. Signatures create a related integrity problem. If signature schemes, root keys, issuer keys, or ledger anchors later lose assurance value, the evidentiary status of earlier records may become contested. Quantum resilience therefore requires separate treatment of confidentiality horizons, integrity horizons, and evidentiary horizons.

The G7 Central Bank Quantum Technologies Working Group's non-prescriptive analytical report reinforces this distinction. It treats HNDL as a present-day confidentiality concern for long-lived financial data and separately identifies authentication, integrity, and non-repudiation risks for tokenized assets, digital identity frameworks, and distributed ledger-based systems. It also frames PQC migration as an operational transition involving cryptographic inventories, compatibility testing, coordination with counterparties and service providers, and coexistence of legacy and quantum-safe standards [16].

At the identity layer, these risks should be assessed as public-key trust-fabric risks, not only as transport-confidentiality risks. HNDL attacks already expose encrypted traffic to future decryption. A future cryptographically relevant quantum computer (CRQC) could also enable the recovery or misuse of exposed issuer, holder-binding, verifier, trust-list, status-list, DID, certificate, DNSSEC, WebPKI, or VDR keys. This could enable forged credentials, impersonated organizations or agents, manipulated status and revocation records, or substituted registry and

semantic metadata [14–16].

Such compromise could undermine legal certainty, disrupt regulated business processes, and weaken trust in public and private digital services. Practical consequences include unauthorized access to sensitive data, fraudulent submissions, invalid compliance evidence, manipulated product or supply-chain records, false organizational authority, and contested audit trails. In high-assurance domains such as defense, law enforcement, public procurement, critical infrastructure, and regulated supply chains, these failures could create operational disruption, liability exposure, and loss of evidentiary value.

AI intensifies the risk landscape. Deepfakes, synthetic documents, voice cloning, and automated fraud campaigns increase the volume and credibility of identity attacks [17]. In organizational settings, AI can be used to forge executive instructions, simulate business partners, manipulate onboarding workflows, or inject false compliance data into digital processes. At the same time, AI agents are becoming operational actors. They trigger transactions, access systems, negotiate within policy limits, and act across organizational boundaries. These agents require persistent identities, explicit authority, and auditable behavior. Identity is therefore both a target of AI-enabled attack and a prerequisite for responsible AI deployment.

Recent controlled evaluations show rapid improvement in AI-assisted cyber capability. Anthropic characterizes Claude Mythos Preview as highly capable in cybersecurity tasks, and the UK AI Security Institute reported improvements on capture-the-flag challenges and multi-step simulated cyber-attack scenarios [18, 19]. A March 2026 cyber-range study evaluated frontier AI models on a 32-step corporate network attack and a 7-step industrial-control-system attack, finding progress across model generations and with greater inference-time compute [20]. These findings should be treated as controlled evidence of improving cyber capability, rather than proof of present real-world autonomous compromise at scale. They support a future risk scenario in which outdated cryptography, unpatched authentication systems, and hidden trust weaknesses become easier for AI-assisted attackers to find and exploit.

The organizational identity problem appears across supply chains, regulated reporting, energy systems, industrial networks, and trusted data-sharing environments. In each setting, the core requirement is reliable proof of who is acting, on whose behalf, with which authority, under which policy, and for which period. These proofs often connect legal identity, delegated authority, compliance status, and the origin of supporting data. The resulting risk is systemic, long-lived, and acute during the transition period. It is systemic because organizational identity depends on many interacting actors; long-lived because records, credentials, and trust anchors may remain relevant for years; and transition-sensitive because migration to PQC must occur while identity systems remain operational. Figure 3 complements this view with selected risk, resource, direct infrastructure, DLT-dependent VDR, deprecation, and completion anchors for corridor prioritization.

Trust-anchor concentration creates additional risk. Many identity ecosystems still depend on a small number of certificate authorities, issuer keys, registry operators, or cloud services. This concentration increases both operational and cryptographic risk. The concern becomes more serious when ledger-based or registry-based proofs are treated as high-value trust anchors for multiple sectors. If the supporting keys, registries, or validation procedures remain on weak or inflexible cryptographic profiles, compromise can cascade across dependent services. Quantum resilience therefore requires diversity of trust anchors, controlled rotation procedures, and visibility into hidden dependencies. Recent roadmaps from direct infrastructure providers point to a compressed planning horizon: Google has set a 2029 PQC migration timeline and explicitly prioritizes authentication services and digital signature migration; Cloudflare targets full post-quantum security, including authentication, by 2029 [21, 22]. These targets are not regulatory deadlines, but they affect interoperability assumptions for corridor participants that depend on

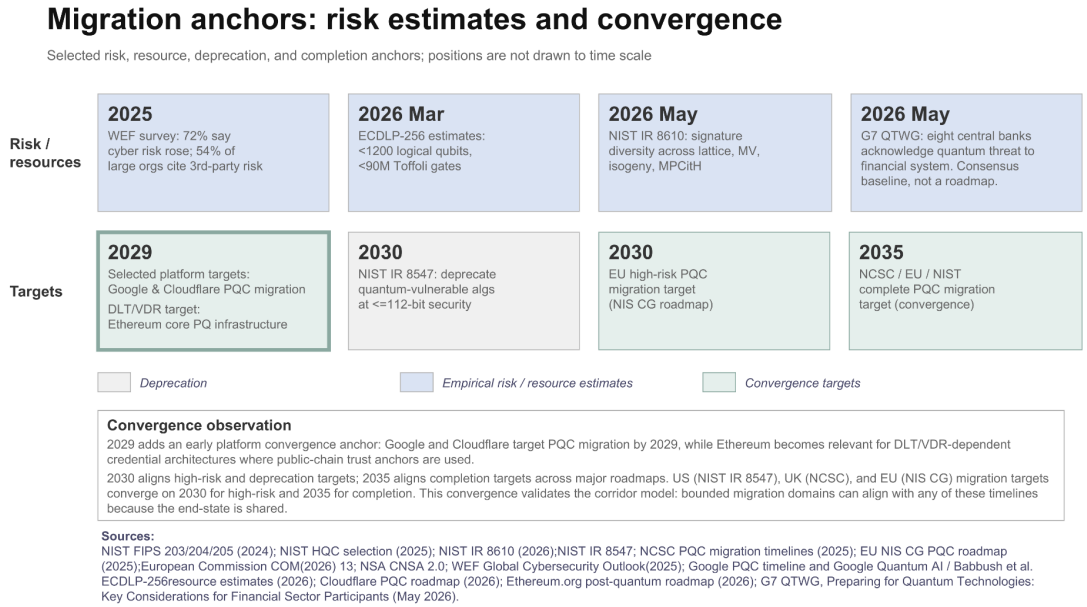

Figure 3: Selected migration anchors for PQC Corridor prioritization. Summary of selected risk, resource, direct infrastructure, DLT-dependent VDR, deprecation, and completion anchors. The dates are not drawn to scale. The figure is intended as a planning aid for prioritizing bounded migration domains, not as a complete timeline of post-quantum cryptography policy or implementation activity.

global cloud, authentication, DNS, content-delivery, security, or network infrastructure.

Ethereum should be scoped differently. It is not an operational dependency for most B2B, B2G, G2G, M2M, supply-chain, procurement, or reporting corridors. It matters where credential ecosystems use Ethereum or Ethereum-based systems as part of a VDR, ledger anchor, or trust-anchor layer. Ethereum's public roadmap targets completion of core post-quantum infrastructure by approximately 2029, while noting that full execution-layer and ecosystem migration extends beyond that date [23]. If robust PQC migration succeeds, Ethereum-based anchoring could become relevant for PQC-resilient or hybrid VDR models, especially in cross-jurisdiction trust infrastructures where one jurisdiction does not fully rely on another jurisdiction's registry, ledger, or VDR. Such models may combine public-chain anchors with national or sectoral trust registries. Google's related disclosure work on ECDLP-256 vulnerabilities in cryptocurrency systems illustrates more broadly that public-chain ecosystems can expose long-lived signature and public-key dependencies that require coordinated PQC migration rather than isolated key replacement [24].

3 Legal and Regulatory Frameworks

The legal environment for digital identity is diverse. Some frameworks are mandatory and operational. Others provide principles, ethical guidance, or technical direction. For quantum-resilient organizational identity, the central question is how these layers interact. The question is whether identity credentials can continue to be issued, verified, supervised, and legally relied upon while the underlying technology changes [6, 7].

The European Union currently provides the most developed binding framework. Regulation

(EU) No 910/2014, as amended by Regulation (EU) 2024/1183, establishes the European Digital Identity Framework and expands the role of wallets, trust services, and electronic attestations of attributes [10]. The framework is relevant for organizational identity because it addresses both natural and legal persons and links identity assurance to supervised trust services. Qualified signatures, qualified seals, timestamps, electronic registered delivery services, and other trust services confer legal effects relevant to business transactions, regulatory reporting, and evidentiary records.

The European Digital Identity Framework also supports wallet-based credential models. Legal-entity interactions often require a combination of attributes, including legal existence, registration data, representation rights, sectoral licenses, and procedural mandates. A wallet architecture can package these claims into reusable and policy-bound credentials. The European Business Wallet proposal is therefore used here as the European reference point for the broader business-wallet pattern [8].

The amended eIDAS regime also creates a legal basis for stronger verification infrastructure. It recognizes electronic ledgers and introduces requirements for qualified electronic ledgers. Commission Implementing Regulation (EU) 2025/2531 sets reference standards and specifications for qualified electronic ledgers [11]. The Commission's digital identity implementation materials describe the purpose of these specifications as ensuring integrity and accurate chronological ordering of electronic data records [9]. This development matters because organizational identity ecosystems require shared verification layers for key bindings, credential status, revocation, chronology, and auditability.

For EU financial-sector corridors, the Digital Operational Resilience Act (DORA) creates additional compliance drivers for PQC migration by requiring financial entities to address ICT risk management, ICT third-party risk, incident reporting, and operational resilience testing [25].

Beyond Europe, the global landscape is more fragmented. Sector-specific coordination is emerging, but it remains limited. The G7 Cyber Expert Group financial-sector roadmap provides a non-binding coordination instrument for PQC migration that emphasizes risk-based sequencing, harmonization across jurisdictions, vendor and third-party dependency management, and ongoing monitoring and recalibration [26]. The United Nations Legal Identity Agenda provides a rights-based and inclusion-oriented foundation for identity through Sustainable Development Goal 16.9 and related work on legal identity and civil registration [27]. UNESCO contributes an ethical framework for AI, data governance, transparency, and human oversight that is relevant for identity systems using biometrics, fraud analytics, and automated decision support [28]. The World Bank's ID4D work emphasizes inclusion, privacy, and trusted digital identification within broader service stacks [29]. The ITU provides implementation-oriented guidance for scalable and interoperable digital identity systems [30]. These frameworks are influential, yet they do not create a unified cross-border trust regime for organizational identity.

This gap is especially visible in legal-person identity, representation, and delegation. Global commerce depends on proving that an organization exists and that a given person, service, or agent is authorized to act on its behalf. Jurisdictions differ on company registration, representation law, evidentiary rules, and supervisory arrangements. Organizational identity is often resolved through sector-specific onboarding, repeated document exchange, or private contractual trust. This is inefficient in stable settings and fragile in fast-moving cross-border settings.

The LEI system offers one partial response. The Legal Entity Identifier provides a global identifier for legal entities and is governed through a recognized data and accreditation structure [12]. The verifiable LEI extends this model into verifiable credentials issued by Qualified vLEI Issuers under the GLEIF governance framework [13]. Verifiable LEIs can support baseline legal-entity identification and selected role assertions across jurisdictions where richer wallet frameworks are not yet mutually recognized. They do not replace industry-specific credentials,

legal requirements, or national rules for evidence. They can, however, reduce friction and improve early interoperability.

Three implications follow. Europe currently offers the strongest legal pathway for wallet-based organizational identity tied to supervised trust services. Global frameworks provide important principles for rights protection, inclusion, ethics, and interoperability, yet they stop short of mutual recognition for business identity and delegation. Near-term cross-border trust for organizations will likely depend on layered arrangements that combine jurisdiction-specific wallets, sectoral credentials, verifiable LEIs, and qualified or contractually governed verification services. This layered model supports corridor-based migration because corridors can test how these components work together before wider deployment.

From an engineering perspective, legal frameworks imply concrete design choices. Assurance levels define how identity is verified and how credentials are created, used, and maintained. Trust services cover signing, sealing, timestamping, validation, and incident response procedures. Wallet frameworks deal with credential formats, selective disclosure, and secure presentation interfaces. Quantum transition planning therefore requires coordinated legal and technical workstreams. A technically elegant migration path can fail if legal recognition of the resulting records is unclear. Conversely, strong legal effect without crypto-agile implementation produces only formal assurance.

4 Business Wallets, Quantum-Safe Digital Public Infrastructure, and qVDRs

This section defines the components required for quantum-resilient organizational identity. The business wallet is the organizational interface for credentials, signatures or seals, secure exchange, and delegated authority. The qVDR is the registry and verification substrate for identifier resolution, issuer and key binding, credential status, revocation, chronology, integrity proofs, and auditability. Together, wallets, qVDR functions, and supporting trust services form part of quantum-safe digital public infrastructure.

4.1 Definitions

Digital public infrastructure is often described in terms of identity, payments, and data exchange. In operational terms, these functions depend on reusable trust components, including credential wallets, trust lists, status registries, revocation services, timestamping, secure messaging, validation services, and audit trails. Quantum-safe digital public infrastructure, or qDPI, refers to the design and governance of these components so that they remain crypto-agile, legally reliable, and interoperable over time.

These definitions follow the self-sovereign identity, or SSI, and decentralized identity role model. Trust is expressed through issuers, holders, verifiers, verifiable credentials, verifiable presentations, and verifiable data registries rather than through one central identity provider.

An issuer is an entity authorized to make claims and issue a verifiable credential. In organizational identity, issuers may include business registers, trust service providers, certification bodies, competent authorities, ecosystem authorities, sector registries, or other governed sources.

A holder is the legal entity, or an authorized representative, service, device, or AI agent acting under its governance, that controls the business wallet and creates verifiable presentations. In this article, holder should not be read as a private individual by default. The holder function is controlled by the organization through governance, policy, delegated authority, and key custody.

A verifier is the relying party that receives a credential or verifiable presentation and checks issuer authority, cryptographic proof, holder binding, credential status, revocation, and policy fit before relying on it. A verifiable credential is a tamper-evident set of claims and metadata whose authorship and integrity can be cryptographically verified. A verifiable presentation is the holder-controlled disclosure of one or more credentials to a verifier.

Revocation is the withdrawal or suspension of a credential, mandate, key binding, or authorization. It is checked through credential-status, registry, or qVDR functions and should be auditable, timely, and privacy-preserving. Verification checks cryptographic proof, status, and conformance. Validation applies the verifier's legal, business, and policy rules to decide whether the result is fit for the intended use.

A business wallet is a wallet-based identity environment for legal entities, their authorized representatives, and, where relevant, software agents and devices acting under their authority. It can hold credentials for legal identity, registrations, licenses, representation rights, customs roles, product claims, sustainability attestations, and data-access authorizations. It can also support electronic signatures, electronic seals, and encrypted communication. The proposed European Business Wallet is one important regulatory example of this general model, and the EU Digital Identity Wallet framework provides the wider policy context for wallets used by citizens, residents, and businesses [8, 9].

The term qualified Verifiable Data Register, a qVDR, is used in this article as a functional concept. It denotes a high-assurance verification registry that may, in European implementations, draw on qualified trust services or qualified electronic ledger infrastructure where applicable legal requirements are met. qVDR should not be read as a separate legal category under eIDAS. This distinction preserves legal accuracy while allowing a systems-architecture discussion of verification infrastructure. A qVDR is the corresponding registry and evidence substrate. It anchors or resolves identifier-to-key bindings, issuer metadata, credential status, revocation records, chronology, and integrity proofs. In Europe, qualified electronic ledgers may support some of these functions where eIDAS requirements are met [10, 11]. In other jurisdictions, comparable functions may be implemented through sectoral registries, contractual trust frameworks, or other governed infrastructure. The functional requirement remains the same: verifiers need reliable status, origin, integrity, and audit information over time.

4.2 Impact

The value of business wallets is clearest in process-intensive and open ecosystems. In a regulated supply chain, a company may need to show that it legally exists, is authorized to manufacture, meets product standards, and has authority to sign documents across counterparties and jurisdictions. In public procurement, an economic operator may need to present company credentials, official attestations, powers of attorney, and evidence of compliance. In digital product passport settings, firms need controlled access to product, conformity, and sustainability data. A business wallet can hold these credentials in reusable form and present them under policy control.

Decentralized identity is useful where regulated participants do not share one identity provider or a fixed federation. It allows trust to be established at interaction time in accordance with Zero Trust Architecture Principles, i.e. never trust, always verify. Before sensitive data is shared or access is granted to an API, machine service, or agentic service, the verifier can authenticate wallet control and authorize the requested action against verified claims, such as legal existence, representation rights, licenses, certifications, mandates, or data-access rights.

This accelerates bilateral onboarding, improves continuous compliance monitoring, limits unnecessary disclosure, and supports cross-organizational trust without forcing all parties into one

central identity system. It is also relevant for agentic services: an AI agent, workflow engine, machine, or API client can act only within a credentialed and policy-bound mandate. The result is a clearer accountability chain: who acted, for which organization, under which authority, for which purpose, and during which period.

The relationship between business wallets and qDPI is reciprocal. Business wallets give organizations an interface for credential storage, presentation, signing, sealing, delegated authority, and secure communication. qDPI gives those wallets a stable trust environment through registry functions, trust anchors, policy resolution, verification and validation services, revocation, and audit support. Without a wallet interface, organizational identity remains fragmented across portals, PDFs, and bilateral onboarding routines. Without verification infrastructure, wallets remain difficult to rely on at scale.

Interoperability will likely develop through a layered architecture rather than a single global standard. At the credential layer, wallets may carry jurisdiction-specific credentials for business registration, tax status, licenses, or public-law mandates. At the cross-jurisdiction layer, they may rely on shared identifiers, portable credential models, bridge credentials, and common secure messaging patterns. At the registry and verification-substrate layer, qVDRs or equivalent services provide resolution, integrity, status, and revocation checks. Within this model, LEIs and vLEIs can serve as bridge credentials where richer mutual recognition remains incomplete [12, 13].

This architecture also supports long-lived secure communication. In DID-based systems, keys for authentication and key agreement can be resolved through DID documents or equivalent registry objects [14]. DIDComm is one relevant protocol family for authenticated and encrypted messaging between DID-controlled parties [31]. If resolution paths, key lifecycles, and messaging profiles are crypto-agile, business wallets can support more durable and HNDL-resilient channels for data sharing, regulatory submissions, and inter-organizational coordination. This matters because supply-chain and public-procedure records often remain sensitive or evidentiary for many years.

4.3 Existing Standards and Future Development

Existing W3C decentralized identity standards are a strong base for crypto agility and PQC-ready identity infrastructure. DID documents support multiple verification methods and purpose-specific key relationships for authentication, assertion, key agreement, capability invocation, and capability delegation [14]. Verifiable Credential Data Integrity supports proof sets and proof chains, which can be used for multi-signature and approval-chain verification [15]. These features allow classical, hybrid, and post-quantum keys and proof suites to coexist during migration. They do not make current deployments quantum-safe by themselves. PQC readiness still depends on approved cryptographic profiles, secure key custody, lifecycle rules, revocation, and corridor governance.

Standardization is part of the architecture. Emerging European work on electronic ledger trust services, ITU material on electronic ledgers in the eIDAS revision, and ISO reference architecture work for blockchain and distributed ledger technologies provide relevant reference points for qVDR-like infrastructures [32–34]. EBSI provides another European example of cross-border verifiable credential infrastructure and trusted organizational registries [35]. These sources do not define qVDR as used here, yet they show that the verification layer is becoming a recognized infrastructure concern.

A practical qDPI program should start from business use cases. It should identify interactions that require trusted identity and delegated authority, map the supporting wallet and registry components, and define how they can evolve cryptographically without breaking interoperability or legal reliance. This leads to the bounded coordination model developed next.

5 PQC Corridors as a Repeatable Migration Framework

The central governance challenge in quantum-resilient identity is coordination. Technical standards alone do not solve migration because identity ecosystems are constrained by network effects. The value of a migrated identity function depends on whether counterparties, wallets, registries, trust-service providers, and verifiers can recognize and process upgraded trust material. Early movers face disproportionate cost and interoperability risk while late movers leave residual exposure across the ecosystem, creating a collective-action problem.

PQC Corridors mitigate this coordination failure by creating a minimum viable trust network in which critical actors migrate together within a bounded operational domain under defined governance. A PQC Corridor is a governance and technical migration domain in which a predefined set of actors agrees on the corridor scope, legal and organizational assurance requirements, data and evidence horizons, trust boundaries, cryptographic migration profile, and operational controls for a defined use case. The corridor also generates reusable evidence outputs, but those outputs are consequences of operating the corridor rather than parameters of its definition.

To make the model concrete, consider a cross-border corridor for dual-use industrial-control equipment, such as a controller used in a power-grid substation. The item is commercially supplied, but it is sensitive because diversion, forged approvals, or false installation authority or leakage of sensitive data to nation threat actors could affect critical infrastructure. The manufacturer, exporter, logistics provider, customs authority, export-control authority, system integrator, and critical-infrastructure operator must verify each other before technical, licensing, routing, and end-use data are exchanged. The corridor must define who may participate, which credentials and trust anchors are accepted, how long approvals and audit evidence must remain reliable, and which hybrid or post-quantum profiles protect signatures and secure messaging.

This can be formalized as $C := \langle S, A, L, H, B, K, O \rangle$. In this representation, S denotes the bounded scope, including the use case, jurisdictions, sectoral context, legal effects, and process limits. A denotes participating actors and their roles, including organizations, ecosystem authority bodies, wallet providers, registry operators, trust-service providers, relying parties, and competent authorities. L denotes legal and organizational assurance requirements, including representation rights, delegated mandates, applicable policies, compliance duties, liability allocation, and recognition conditions. H denotes the data and evidence horizon, including confidentiality lifetimes, integrity requirements, and evidentiary validity periods. B denotes the trust boundary, including accepted credentials, trust anchors, issuer lists, status services, and verification services. K denotes the cryptographic migration profile, including classical, hybrid, and post-quantum algorithms, key lifetimes, algorithm-lifecycle rules, downgrade resistance, and deprecation. O denotes operational controls, including issuance, monitoring, status and revocation management, telemetry, incident handling, rollover, degraded-mode operation, and continuity. Figure 4 visualizes this formal structure and the separate evidence function.

The evidence output is modeled separately as $E(C) := \text{evidence}(C)$. E(C) denotes the reusable evidence produced by operating the corridor, such as audit records, procurement clauses, conformance tests, trust-anchor rotation procedures, telemetry requirements, and operational runbooks. The validity condition is $\text{valid}(C)$ if and only if L, B, K, and O remain mutually consistent over H. This condition makes explicit that legal assurance, accepted trust material, cryptographic choices, and operational controls must remain coherent for the period during which data, credentials, and evidence remain relevant.

Corridors convert an open ecosystem transition into a governed implementation sequence. They reduce uncertainty by aligning scope, assurance, trust material, cryptographic migration, operational controls, and evidence generation where risk and operational need are highest, without waiting for universal readiness.

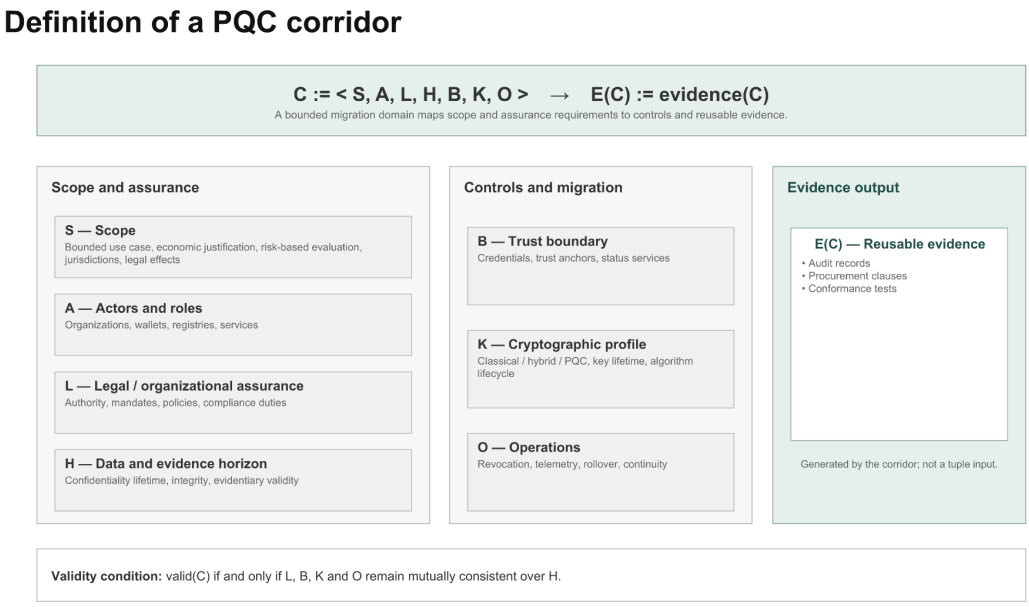

Figure 4: Formal definition of a PQC Corridor. A PQC Corridor is represented as $C := \langle S, A, L, H, B, K, O \rangle$, where scope, actors, legal or organizational assurance, data and evidence horizons, trust boundaries, cryptographic profiles, and operational controls are jointly governed. The evidence function $E(C) := \text{evidence}(C)$ denotes reusable outputs generated by corridor operation, including audit records, procurement clauses, conformance tests, telemetry requirements, and operational runbooks. The validity condition requires legal assurance, trust boundaries, cryptographic profiles, and operational controls to remain mutually consistent over the relevant data and evidence horizon.

The corridor model is particularly well suited to organizational identity. Many business processes have clear boundaries, defined participants, formal liabilities, and defined data flows, which makes S, A, L, H, B, K, and O observable and governable. These characteristics allow corridors to be built around sensitive or high-value interactions such as customs declarations, dual-use goods export documentation, public procurement, regulated incident reporting, energy flexibility markets, controlled sharing of industrial compliance data, trade-documentation flows, financial-compliance attestation channels, and cross-border health-data exchange. In each case, an ecosystem authority body or equivalent governance function defines rules and conformance expectations, business wallets provide the organizational interface, qVDRs or equivalent registries support resolution, status, revocation, timestamping, and integrity proofs, and corridor governance coordinates identity, messaging, cryptography, monitoring, and evidence generation.

5.1 Scope, Actors, and Legal or Organizational Assurance (S, A, L)

S, A, and L define the scope and assurance boundary of the corridor.

S defines the bounded use case, jurisdictions, sectoral context, and legal effects of the migration domain. Crucially, S must incorporate a formal economic justification to ensure alignment with business stakeholder requirements and institutional feasibility. This economic dimension validates the resource allocation necessary for PQC transition by balancing the cost of implementation against the long-term value of data assets. Furthermore, S necessitates a rigorous, risk-based evaluation focusing on the potential failure modes of the underlying identity fabric and the subsequent economic value at risk (EVAR) should sensitive data or critical infrastructure be compromised.

A identifies the participating actors and their functional roles within the ecosystem. This includes ecosystem authority bodies, organizations, wallet providers, registry operators, and trust-service providers, as well as relying parties, competent authorities, software services, devices, and autonomous agents where relevant.

L defines the specific requirements attached to the roles identified in A. This encompasses representation rights, delegated mandates, applicable policies, compliance duties, liability allocation, and recognition conditions.

Together, these parameters determine the structural integrity of the corridor, defining whether it relies on qualified trust services, sector-specific regulation, contractual trust, or a hybrid of these mechanisms. The validity of the corridor is predicated on the continuous mutual consistency of these requirements against the established evidence horizon H.

5.2 Data and Evidence Horizon (H)

H defines the data scope and the time horizon over which data, credentials, trust anchors, and records must remain confidential, integral, or evidentially valid. Data with long confidentiality horizons requires early post-quantum or hybrid key-establishment mechanisms. Records with long evidentiary horizons require migration planning for signatures, timestamps, seals, validation data, issuer keys, status records, and trust anchors. H also determines the priority order for migration because short-lived operational data and long-lived regulatory evidence do not carry the same quantum-transition risk.

5.3 Trust Boundary and Credential Controls (B)

B defines the trust boundary of the corridor. It specifies which credentials, issuers, trust anchors, status services, certificate chains, wallet requirements, registry services, delegated-authority models, and bridge credentials are accepted within the corridor. B must remain consistent with L: a trust anchor or credential type is not sufficient if it cannot support the legal or organizational assurance claimed for the use case. For cross-jurisdiction corridors, LEI and vLEI credentials can provide a baseline legal-entity anchor, while sector-specific credentials carry richer product, license, conformity, sustainability, or filing-authority claims [12, 13].

5.4 Cryptographic Profile and Operational Controls (K, O)

K and O define the control side of the corridor.

K specifies approved algorithms, classical, hybrid, and PQC modes, downgrade resistance, key lifetimes, secure messaging rules, algorithm-lifecycle rules, and deprecation procedures.

O specifies issuance, onboarding, monitoring, status and revocation management, telemetry, incident handling, key or trust-anchor rollover, degraded-mode operation, and business continuity. The corridor should be able to rotate algorithms and keys without breaking interoperability or legal reliance. This requires telemetry that detects legacy fallback, governance rules for deprecating profiles, and procurement clauses that require vendor support for migration. The profile should align with emerging PQC standards and wider transition guidance [2–7, 26, 36].

5.5 Evidence Function and Learning Layer (E(C))

The evidence function E(C) defines how corridor operation is captured and reused. Because E(C) is generated by the corridor rather than included as a tuple parameter, it records whether the corridor operated under its agreed scope, assurance, trust-boundary, cryptographic, and operational assumptions. Each corridor should produce reusable evidence, including audit records, monitoring records, procurement clauses, interoperability test cases, conformance profiles, trust-anchor rotation procedures, operational runbooks, telemetry requirements, and incident evidence. These outputs allow successful corridor designs to scale into broader adoption. This learning function distinguishes a corridor from a pilot: a pilot tests whether a technical solution can work, whereas a corridor tests whether a governed migration pattern can operate under real conditions and be repeated across sectors and jurisdictions.

Corridors also support resilience and regeneration because they create bounded high-assurance environments and structured feedback loops for later deployment stages. The validity condition links this learning function back to the formal model: if L, B, K, and O drift out of mutual consistency over H, the corridor must be corrected, renewed, or retired. The model aligns with wider innovation-ecosystem and quantum-readiness initiatives that seek to move from strategic awareness to operational implementation [37, 38].

Three design principles follow from the corridor model. Minimal identity exposure means that participants exchange only the claims required by S and L. Selective disclosure, role scoping, and limited retention reduce attack surface and governance overhead. Risk-based PQC prioritization starts from H: migration begins with assets that have long confidentiality, integrity, or evidentiary horizons, including organizational credentials, secure messaging channels, trust anchors, and evidentiary records. Proportionate governance means that B, K, and O must provide accountability, interoperability, and auditability while remaining operationally manageable. Excessive procedural overhead delays coordination, while weak governance creates hidden systemic risk.

A cross-border corridor for export-controlled industrial-control equipment illustrates the model. Returning to this sensitive-goods corridor, the tuple maps as follows. S would define the export, transport, installation, and service use case across participating jurisdictions, including process limits and legal effects. A could include the manufacturer, exporter, importer, logistics operator, customs authority, export-control authority, conformity assessment body, system integrator, wallet providers, registry operators, and the critical-infrastructure operator. L would specify representation rights, export authorizations, end-use attestations, recipient eligibility, handling duties, access policies, and recognition conditions. H would cover the confidentiality, integrity, and evidentiary horizons of technical data, license records, shipment records, end-use evidence, and service mandates. B would specify accepted business wallet credentials, vLEI or other bridge credentials where needed, issuer discovery, credential status verification, revocation, and chronological integrity services [12, 13]. K would require hybrid or post-quantum profiles for signatures and secure messaging during migration. O would define onboarding, telemetry, incident handling, revocation monitoring, continuity, and trust-anchor rollover. Figure 5 shows this logic as a simplified cross-border corridor instance involving two jurisdictions.

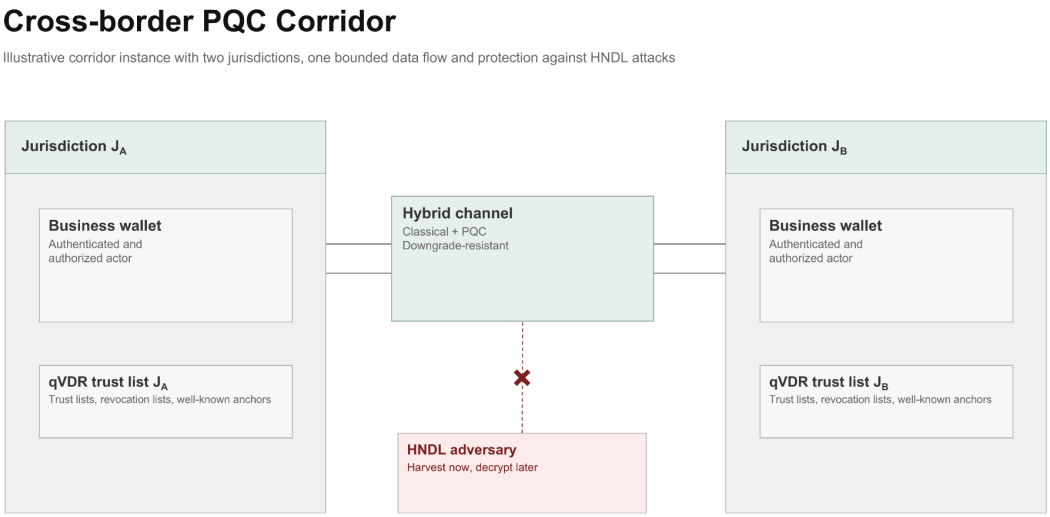

Figure 5: Illustrative cross-border PQC Corridor. The figure shows a bounded corridor instance between two jurisdictions. Each jurisdiction uses business wallets and qVDR-based trust lists to support actor authentication, authorization, credential status, revocation, and trust-anchor validation. The cross-border data flow uses a downgrade-resistant hybrid channel combining classical and post-quantum protection to reduce harvest-now, decrypt-later exposure during the migration period.

The same formalization can also be applied to public-sector channels. In a cross-border B2G reporting corridor, S would define the reporting procedure, jurisdictions, submission channel, and legal effects; L would define official roles and filing authority; B would identify accepted business wallet credentials, qualified trust services, timestamps, seals, registered delivery, and registry dependencies; K would define the cryptographic migration profile; and O would define validation, monitoring, status and revocation management, archiving, audit, incident response, and trust-anchor rotation. These examples show that PQC Corridors are not confined to one industry. They provide a general migration framework for organizational identity and government interactions wherever legal effect, interoperability, and cryptographic resilience are required.

6 Adoption Challenges and Implementation Pathways

The main barriers to quantum-resilient identity are institutional and organizational as well as technical. Long-term risks are often underestimated in budget and procurement cycles. Identity infrastructures are deeply embedded in business processes, while vendor contracts create lock-in and supervisory requirements vary across jurisdictions. Together, these factors slow down migration even when the technical direction is clear.

A second barrier is conceptual. Because many organizations still view digital identity through a narrow authentication lens, they overlook the broader role of identity in organizational representation, secure exchange, compliance automation, and auditability. If identity is framed only as login infrastructure, quantum migration appears as a specialized security task. If identity is framed as an organizational trust layer, migration becomes an enterprise risk concern linked to continuity, legal effect, and ecosystem position.

A third barrier is the use of centralized shortcuts in the name of sovereignty or decentralization. Some deployments rely on fragile dependencies such as live web resolution, single-provider wallet services, or narrow cloud chokepoints. These choices may accelerate early deployment, yet they can weaken resilience in contested or degraded operating conditions. Corridor design should therefore address offline validation paths, controlled dependency mapping, and the ability to maintain trust during partial network or service failure.

6.1 Governance and Visibility

Implementation should begin with executive ownership, ecosystem-level governance, and technical asset visibility. A board or executive committee should classify quantum-resilient organizational identity as a strategic risk and infrastructure issue, creating a mandate for cross-functional coordination across security, architecture, legal, procurement, privacy, product, and operations. The first operational deliverables should be a Cryptographic Bill of Materials and a Trust Anchor Bill of Materials. These inventories should map algorithms, certificates, issuer keys, registry dependencies, wallet dependencies, status services, revocation services, monitoring channels, and secure messaging channels. They should also link each asset to confidentiality horizons, integrity horizons, and evidentiary requirements.

Where a corridor spans multiple organizations or jurisdictions, governance should be assigned to an Ecosystem Authority Body or an equivalent authority function. The term is used here as a functional concept, not as a separate legal category. It may begin as a cross-jurisdictional PQC project organization that coordinates regulators, trust-service providers, registry operators, wallet providers, relying parties, and sector participants. As the corridor matures, it can become a continuous governance function that maintains rules, policies, conformance requirements, conformance assessment, accepted issuers, monitoring duties, status and revocation policies, and escalation paths. Its role is to keep L, B, K, and O mutually consistent over H and to decide when corridor profiles should be corrected, renewed, or retired.

6.2 Risk-Based Corridor Launch

The next phase is to select the first PQC corridor on a risk basis. Priority should be given to use cases where organizational credentials, secure communications, registry services, or evidentiary records must remain confidential, authentic, and legally reliable over long periods. Strong candidates include sensitive government-to-government communications, defense and law-enforcement communications, regulated supply-chain compliance, cross-border B2G reporting,

dual-use goods export documentation, controlled industrial data sharing, public procurement, and product passport ecosystems.

Corridor selection should combine damage potential with implementation control. The first corridor should be important enough to justify early PQC migration, but narrow enough to limit operational risk. Selection criteria should include: high impact if trust fails; long confidentiality, integrity, or evidentiary horizons; clear trust boundaries; a limited set of actors, credential types, registries, and protocols; controlled status and revocation mechanisms; rollback and parallel-operation options; and reusable evidence value for later migrations.

Launch mechanics should be explicit. The corridor team should define the minimal viable scope, name the participants and authority function, freeze the first credential and trust-anchor baseline, select the hybrid or post-quantum profile, set downgrade and fallback rules, test issuance, presentation, verification, status, and revocation flows, and operate in parallel with legacy channels before expanding the scope.

The initial scope should be treated as a minimal viable corridor. It should start with a confined participant group, a simple use case that can be pragmatically implemented, a small number of high-value credentials or records, defined trust anchors, explicit assurance requirements, and measurable exit criteria. Expansion should be phased by adding actors, extending scope, credential types, registries, protocols, legal effects, and jurisdictions only after interoperability, telemetry, incident handling, and revocation have been tested under corridor conditions.

6.3 Supply-Chain Alignment and Scaling Through Evidence

Corridor migration requires supply-chain alignment. Hardware roots of trust, entropy sources, HSMs, secure elements, wallet software, cloud services, registry operators, and managed service providers all shape corridor resilience. Migration requirements should therefore be reflected in procurement, certification, service-level design, and the production of reusable evidence outputs.

Where mutual recognition is incomplete, vLEIs can provide the interim legal-entity anchor described above [13].

Migration also requires clearer metrics. Boards and program teams need leading indicators that show whether residual exposure is decreasing. Useful metrics include the share of long-lived identity data flows moved to crypto-agile profiles, the number of trust anchors covered by rotation procedures, the proportion of business wallet interactions that can be verified without legacy fallback, and the number of vendors that meet corridor requirements. Procurement language should reinforce these metrics by requiring algorithm agility, documented key-lifecycle controls, and interoperability testing under corridor conditions.

7 Systems Architecture for Quantum-Resilient Organizational Identity

Quantum-resilient organizational identity for a digital data-sharing corridor should be implemented as an integrated governance and technical stack rather than as a set of isolated layers. Figure 6 summarizes the architecture. Its top-to-bottom sequence is: ecosystem authority body; trusted sources; trust services and credential issuance; business wallet or European Business Wallet; secure organizational data exchange; and Verifiable Data Registry, or qVDR. Monitoring, status management, and revocation operate as feedback functions across the stack. The architecture operationalizes the formal corridor model $C := \langle S, A, L, H, B, K, O \rangle$: the ecosystem authority body governs S, A, L, B, K, and O; trusted sources ground L and B; trust services and

issuance bind L, B, K, and O into credentials; wallets operationalize B; secure data exchange implements O; qVDR functions provide registry, status, and evidence inputs for E(C); and H determines migration priority, evidence retention, and validity over time.

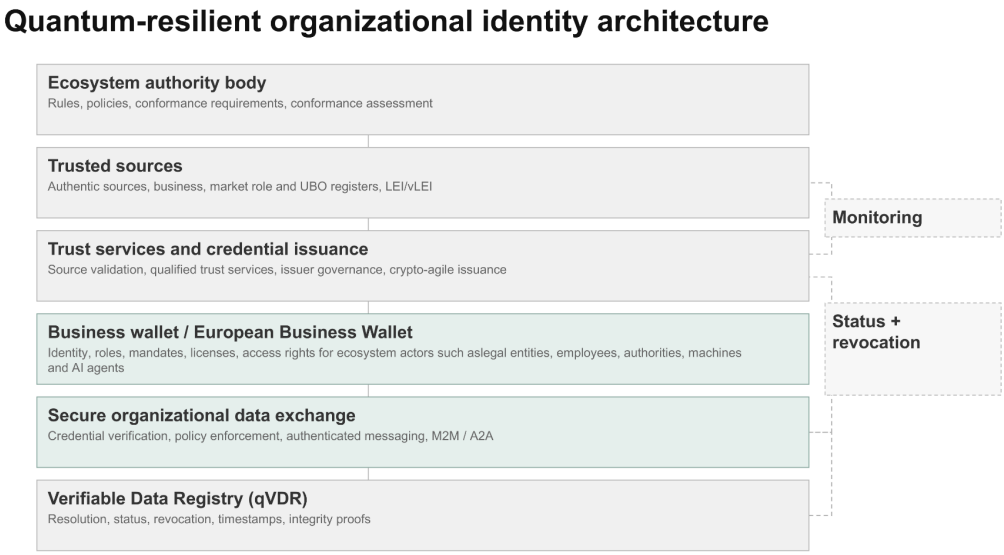

Figure 6: Quantum-resilient organizational identity architecture. The architecture organizes quantum-resilient organizational identity as a governance and technical stack. The ecosystem authority body defines rules, policies, conformance requirements, and assessment processes. Trusted sources and trust services support credential issuance and legal or organizational assurance. Business wallets operationalize credentials for organizations, employees, authorities, machines, and AI agents. Secure organizational data exchange performs credential verification, policy enforcement, authenticated messaging, and M2M or A2A interaction. The qVDR provides registry, status, revocation, timestamping, and integrity-proof functions, while monitoring and revocation operate as feedback mechanisms across the stack.

7.1 Ecosystem Authority Body

The ecosystem authority body is the governance function at the top of the architecture. It may start as a cross-jurisdictional PQC project organization and mature into continuous governance for a corridor or a family of corridors. It defines rules, policies, conformance requirements, accepted credential families, cryptographic profiles, monitoring duties, status and revocation policies, and conformance assessment procedures. The term is used here as a functional concept rather than as a separate legal category.

At corridor level, the ecosystem authority body makes S, A, L, B, K, and O explicit and keeps L, B, K, and O mutually consistent over H. It need not operate every technical component. Its role is to set the conditions under which issuers, wallet providers, registry operators, trust-service providers, relying parties, and competent authorities can interoperate and be assessed.

Where the ecosystem authority body also operates registry, trust-service, or assessment functions, conformance assessment of its own governance and controls should be independent from those operational functions.

7.2 Trusted Sources

Trusted sources ground legal and organizational assertions before credentials are issued. They include authentic sources, business registers, market-role registers, beneficial-ownership registers, LEI and vLEI sources, sector registries, and other competent data sources. These sources do not by themselves create portable organizational credentials. They provide the evidence basis used by trust services and issuers.

Trusted sources therefore connect identity, authority, role, and compliance claims to the corridor's assurance requirements and trust boundary. The data and evidence horizon, H, determines how long those records, or evidence derived from them, must remain reliable for confidentiality, integrity, and evidentiary purposes.

7.3 Trust Services and Credential Issuance

Trust services and credential issuance translate source validation and ecosystem rules into wallet-usable credentials. Qualified trust services, accredited issuers, certification bodies, and governed credential issuers may validate source data, bind subject identifiers, define assurance levels, sign or seal credential material, create status endpoints, and support renewal or re-issuance.

For organizational identity, issuance must cover more than the existence of a legal entity. It may also include representation rights, delegated mandates, sectoral licenses, compliance status, device identity, software-service identity, or authority granted to an AI agent. Where cross-jurisdiction recognition is incomplete, LEI and vLEI credentials can provide a baseline legal-entity anchor while richer credentials carry jurisdiction-specific or sector-specific claims [12, 13].

Issuance also defines the technical and evidentiary properties of a credential. These include the credential format, semantic model, issuer identifier, subject identifier, validity period, assurance level, status mechanism, revocation semantics, cryptographic profile, and evidence horizon. In a quantum-transition setting, these properties should be crypto-agile from the outset and should support protection against future forgery, long-term integrity, and the non-repudiation value of credentials and related evidence. These choices link assurance, accepted trust material, algorithm profile, and lifecycle controls, so L, B, K, and O must be defined together [2–4, 36].

7.4 Business Wallet / European Business Wallet

The business wallet layer is the organizational control point for issued credentials. It stores credentials and controls presentation to counterparties, authorities, services, machines, and AI agents. It should support selective disclosure, policy-bound presentation, electronic signatures or seals, secure key storage, controlled use of secure key material, and interfaces to status and revocation services.

Within a corridor, the wallet is the usable part of the trust boundary. It must respect the assurance requirements and evidence horizon defined for the use case. The proposed European Business Wallet illustrates this model in a regulated European form [8, 9].

7.5 Secure Organizational Data Exchange

Secure organizational data exchange is the operational layer in which credentials are presented, verified, and used to authorize data sharing, reporting, and M2M or A2A processes. It includes credential verification, policy enforcement, authenticated messaging, secure APIs, DIDComm or

equivalent protocols, and logging for audit and evidence. DIDComm offers one relevant model for authenticated and encrypted messaging between DID-controlled parties [31].

Verification in this layer is an operational access-control act. A verification module checks credential presentations against the applicable access policy and calls the qVDR or equivalent registry services for identifier resolution, credential status, revocation records, timestamps, semantic references, and integrity proofs. AI agents, workflow engines, and autonomous services should operate through the same policy-bound exchange layer, with runtime verification of identifiers, credentials, delegated authority, and access rights. This is where operational controls become access decisions, exchange logs, and evidence for the relevant horizon.

7.6 Verifiable Data Registry (qVDR), Monitoring, Status, and Revocation

The qVDR sits at the registry and evidence substrate of the architecture. It supports identifier resolution, credential status, revocation records, timestamping, integrity proofs, issuer metadata, and audit inputs. W3C DIDs provide one way to structure identifier control and key discovery [14]. The qVDR concept describes a high-assurance environment for maintaining these bindings and status checks over time, whether implemented through qualified trust services, qualified electronic ledgers, or governed sector registries. It should not be read as a separate legal category under eIDAS. These qVDR functions anchor the trust boundary, support operations, and feed corridor evidence.

Monitoring, status management, and revocation are feedback functions across the architecture. Monitoring should detect issuer-key changes, algorithm fallback, expired or suspended credentials, registry unavailability, revocation delays, policy drift, and failures in cryptographic or operational controls. Status and revocation services should allow credentials, mandates, trust anchors, and access rights to be suspended, withdrawn, renewed, or re-issued without breaking the wider corridor.

Controlled offline or degraded-mode verification remains important. In logistics, industrial operations, crisis response, and cross-border public procedures, verifiers may need to rely for a defined period on cached trust lists, portable proofs, signed status information, or equivalent mechanisms. Those degraded-mode rules are operational controls and must remain consistent with assurance, trust-boundary, and cryptographic requirements over the relevant horizon.

7.7 Cross-Cutting Cryptographic and Key-Lifecycle Migration

The cryptographic and key-lifecycle domain is cross-cutting rather than a separate layer in the figure. It applies across trust services, issuance, wallets, exchange, and qVDR operation. Organizational identity depends on how keys are generated, protected, rotated, recovered, and retired. In practice, this may involve software vaults, HSMs, secure elements, trusted execution environments, or multi-party computation. These controls implement the cryptographic profile and must match the confidentiality, integrity, and evidentiary horizons of protected data and credentials.

Algorithm approval does not mitigate implementation risk; consequently, PQC implementations within Hardware Security Modules (HSMs), secure elements, Trusted Execution Environments (TEEs), or Multi-Party Computation (MPC) components must be rigorously evaluated for side-channel vulnerabilities, including timing leakage, power analysis, electromagnetic emissions, and fault injection. Furthermore, the physical constraints of hardware often impede cryptographic agility [39]. To address these limitations, modern software-based paradigms, specifically secure Multi-Party Computation (sMPC), should be prioritized. Such software-defined solutions

facilitate superior agility, as updating cryptographic logic within a controlled software lifecycle is significantly more efficient than the logistical and capital-intensive process of physical hardware replacement.

Quantum resilience requires a planned shift from legacy public-key algorithms to post-quantum signatures and key establishment, typically through hybrid profiles during transition [2–4, 36]. Cryptographic agility should be treated as a design property with clear deprecation rules, telemetry for legacy fallback, and coordinated key rotation. The ecosystem authority body or equivalent governance function should maintain the cryptographic profile and conformance criteria, while issuers, wallets, qVDR services, and exchange services implement them. The corridor model is useful here because it allows K and the related lifecycle controls to be tested across issuance, wallet use, secure exchange, and qVDR-based verification before wider deployment.

8 Strategic Implications for Governance and Implementation

At the board level, quantum-resilient organizational identity should be treated as critical infrastructure. The concern goes beyond basic cybersecurity because it affects legal validity, business continuity, supply-chain trust, and the ability to automate regulated processes. Boards should set limits for HNDL risk, ensure visibility of trust-anchor concentration, and track progress toward crypto-agile profiles for long-term identity data flows.

At the executive level, organizations should establish a cross-functional transition function with authority over security, enterprise architecture, legal, procurement, privacy, product, and operations. This function may take the form of a Quantum Identity Transition Office. Its responsibilities should include tracking cryptographic and trust-anchor assets, planning migration, working with vendors, preparing for incidents, and coordinating across the ecosystem. The transition function should treat organizational identity as a shared infrastructure dependency rather than as an isolated authentication service.

At the technical and procurement levels, organizations should require crypto-agility by design. New identity systems, wallets, registries, secure messaging services, and managed services should support algorithm upgrade paths, documented key-lifecycle controls, interoperability testing, and evidence-producing controls. Procurement should also require support for corridor profiles, telemetry, and trust-anchor rotation procedures. These requirements reduce the risk of building new systems that need replacement before the end of their lifecycle.

At the ecosystem level, organizations should launch PQC Corridors in bounded, high-value settings, using business wallets as the organizational interface and vLEIs as bridge credentials where mutual recognition is incomplete. Each corridor should assign an ecosystem authority body or equivalent governance function to maintain rules, conformance assessment, monitoring duties, status and revocation policies, and profile-renewal procedures. Over time, corridor outputs can inform standards, procurement clauses, conformity assessment, and supervisory practice.

The long-term governance goal is adaptive renewal of the identity trust layer. Identity systems must continue to function during cryptographic change and partial failure while institutional controls are updated in response to incidents, revised trust assumptions, and changing threats and technologies.

9 Conclusion

Digital identity is now a core trust layer of the digital economy. In organizations, it supports identifying companies, managing delegated authority, enabling secure data exchange, ensuring auditability, and coordinating automated systems. Quantum computing and AI-enabled fraud place this layer under structural pressure. The effect is strongest where identity records, trust anchors, and business relationships remain relevant over long periods.

This article argues that the transition cannot be managed through isolated technical upgrades. It requires a governance and systems architecture model aligned with the ecosystem structure of identity. The PQC Corridor is proposed as a repeatable framework for overcoming the network-effect bottleneck in post-quantum transition.

The European Business Wallet illustrates one regulatory direction, while the broader lesson is global: trusted digital interaction in supply chains, public procedures, data-sharing ecosystems, M2M processes, and agent-to-agent environments depends on robust verification infrastructure and governed migration paths.

The near-term task is to identify trust dependencies, prioritize long-term organizational identity assets, and launch corridor-based migration in high-value settings. This approach offers a realistic path toward quantum-resilient and legally meaningful organizational identity.

Appendix A. A Simple Corridor Parameter-to-Artefact Matrix

Table 1 maps the corridor model to implementation artefacts that regulators, auditors, and participants can review when assessing corridor readiness and continued validity.

Table 1: Corridor parameter-to-artefact matrix.

Corridor element	**Implementation artefact**	**Regulator or auditor check**
S - Scope	Scope document	Is the use case, jurisdictional perimeter, legal effect, process limit, and risk or economic justification clear?
A - Actors	Participant and role register	Are all participants, authority functions, issuers, wallet providers, registry operators, service providers, devices, and agents identified?
L - Legal and organizational assurance	Legal-basis and assurance assessment	Are representation rights, mandates, liability allocation, recognition conditions, and compliance duties defined?
H - Data and evidence horizon	Data-classification and evidence-horizon matrix	Are data types and confidentiality, integrity, evidentiary lifetimes, retention duties, and long-term validation needs mapped?
B - Trust boundary	Trust-anchor and credential inventory	Are accepted credentials, issuers, trust anchors, status and revocation services, bridge credentials, and qVDR dependencies listed?
K - Cryptographic profile	Cryptographic profile specification	Are algorithms, hybrid or PQC modes, key lifetimes, downgrade controls, deprecation rules, and implementation-security requirements defined?
O - Operational controls	Operational runbook	Are onboarding, issuance, verification, access policy rules, monitoring, telemetry, incident response, rollover, revocation, degraded mode, and continuity tested?
E(C) - Evidence output	Evidence pack and audit trail	Are audit records, conformance tests, procurement clauses, telemetry records, incident evidence, and change logs available?
valid(C) - Validity condition	Consistency review and renewal decision	Does the evidence show that L, B, K, and O remain mutually consistent over H, or that the corridor was corrected, renewed, or retired?

References

[1] R. Babbush, A. Zalcman, C. Gidney, M. Broughton, T. Khattar, H. Neven, T. Bergamaschi, J. Drake, and D. Boneh, "Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities: Resource Estimates and Mitigations," arXiv:2603.28846, Mar. 2026. https://arxiv.org/abs/2603.28846

[2] National Institute of Standards and Technology, "Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography," Aug. 13, 2024. https://www.nist.gov/news-events/news/2024/08/announcing-approval-three-federal-information-processing-standards-fips

[3] National Institute of Standards and Technology, "Transition to Post-Quantum Cryptography Standards," NIST IR 8547, Initial Public Draft, Nov. 2024. https://doi.org/10.6028/NIST.IR.8547.ipd

[4] National Institute of Standards and Technology, "Status Report on the Second Round of the Additional Digital Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process," NIST IR 8610, May 2026. https://doi.org/10.6028/NIST.IR.8610

[5] National Cyber Security Centre, "Timelines for Migration to Post-Quantum Cryptography," Mar. 20, 2025. https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

[6] NIS Cooperation Group, "A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography," June 2025. https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

[7] European Commission, "Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2022/2555 as regards simplification measures and alignment with the [Proposal for the Cybersecurity Act 2]," COM(2026) 13 final, Jan. 20, 2026. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52026PC0013

[8] European Commission, "Proposal for a Regulation on the Establishment of European Business Wallets," Policy proposal, Nov. 19, 2025. https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-establishment-european-business-wallets

[9] European Commission, "EU Digital Identity Wallet" and "The European Digital Identity Regulation," 2026. https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/694487738/EU%2BDigital%2BIdentity%2BWallet%2BHome ; https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/915931811/The%2BEuropean%2BDigital%2BIdentity%2BRegulation

[10] European Union, "Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework," Official Journal of the European Union, Apr. 11, 2024. https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng

[11] European Commission, "Commission Implementing Regulation (EU) 2025/2531 of 16 December 2025 laying down rules for the application of Regulation (EU) No 910/2014 as regards reference standards and specifications for qualified electronic ledgers," Official Journal of the European Union, Dec. 16, 2025. https://eur-lex.europa.eu/eli/reg_impl/2025/2531/oj/eng

[12] Global Legal Entity Identifier Foundation, "The Legal Entity Identifier (LEI)," 2026. https://www.gleif.org/en/about-lei/introducing-the-legal-entity-identifier-lei

[13] Global Legal Entity Identifier Foundation, "vLEI Ecosystem Governance Framework," 2026. https://www.gleif.org/en/organizational-identity/become-a-vlei-issuer-qvi/vlei-ecosystem-governance-framework

[14] World Wide Web Consortium, "Decentralized Identifiers (DIDs) v1.0" and "Decentralized Identifiers (DIDs) v1.1," W3C Recommendation, July 19, 2022, and W3C Candidate Recommendation Snapshot, Mar. 5, 2026. https://www.w3.org/TR/did-core/ ; https://www.w3.org/TR/did-1.1/

[15] World Wide Web Consortium, "Verifiable Credentials Data Model v2.0" and "Verifiable Credential Data Integrity 1.0," W3C Recommendations, May 15, 2025. https://www.w3.org/TR/vc-data-model-2.0/ ; https://www.w3.org/TR/vc-data-integrity/

[16] G7 Central Bank Quantum Technologies Working Group, "Preparing for Quantum Technologies: Key Considerations for Financial Sector Participants," Report, May 2026. https://www.bancaditalia.it/media/notizie/2026/G7_Key_Considerations_for_Financial_Sector_Participants_May_2026.pdf?language_id=1

[17] World Economic Forum, "Global Cybersecurity Outlook 2025," Report, Jan. 13, 2025. https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

[18] Anthropic, "Assessing Claude Mythos Preview's Cybersecurity Capabilities," Anthropic Frontier Red Team, Apr. 2026. https://red.anthropic.com/2026/mythos-preview/

[19] UK AI Security Institute, "Our Evaluation of Claude Mythos Preview's Cyber Capabilities," Apr. 13, 2026. https://www.aisi.gov.uk/blog/our-evaluation-of-claude-mythos-previews-cyber-capabilities

[20] L. Folkerts, W. Payne, S. Inman, P. Giavridis, J. Skinner, S. Deverett, J. Aung, E. Zorer, M. Schmatz, M. Ghanem, J. Wilkinson, A. Steer, V. Hong, and J. Wang, "Measuring AI Agents' Progress on Multi-Step Cyber Attack Scenarios," arXiv:2603.11214, Mar. 2026. https://arxiv.org/abs/2603.11214

[21] Google, "Quantum frontiers may be closer than they appear," Mar. 25, 2026. https://blog.google/innovation-and-ai/technology/safety-security/cryptography-migration-timeline/

[22] Cloudflare, "Cloudflare targets 2029 for full post-quantum security," Apr. 7, 2026. https://blog.cloudflare.com/post-quantum-roadmap/

[23] Ethereum Foundation, "Post-quantum cryptography on Ethereum," ethereum.org, May 8, 2026. https://ethereum.org/roadmap/future-proofing/quantum-resistance/

[24] R. Babbush and H. Neven, "Safeguarding cryptocurrency by disclosing quantum vulnerabilities responsibly," Google Research Blog, Mar. 31, 2026. https://research.google/blog/safeguarding-cryptocurrency-by-disclosing-quantum-vulnerabilities-responsibly/

[25] European Union, "Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011," Official Journal of the European Union, Dec. 27, 2022. https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

[26] G7 Cyber Expert Group, "G7 Cyber Expert Group Statement on Advancing a Coordinated Roadmap for the Transition to Post-Quantum Cryptography in the Financial Sector: January 2026," Jan. 13, 2026. https://www.gov.uk/government/publications/advancing-a-coordinated-roadmap-for-the-transition-to-post-quantum-cryptography-in-the-financial-sector/g7-cyber-expert-group-statement-on-advancing-a-coordinated-roadmap-for-the-transition-to-post-quantum-cryptography-in-the-financial-sector-january-20

[27] United Nations Statistics Division, "UN Legal Identity Agenda," 2026. https://unstats.un.org/legal-identity-agenda/

[28] UNESCO, "Recommendation on the Ethics of Artificial Intelligence," Policy recommendation, 2021. https://www.unesco.org/en/artificial-intelligence/recommendation-ethics

[29] World Bank Group, "Principles on Identification for Sustainable Development: Toward the Digital Age," Working paper, 2017. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/368061626756712617

[30] International Telecommunication Union, "Digital Identity Roadmap Guide," Guide, 2018. https://www.itu.int/pub/d-str-digital.01-2018

[31] Decentralized Identity Foundation, "DIDComm Messaging Specification v2.0," Specification, 2022. https://identity.foundation/didcomm-messaging/spec/v2.0/

[32] CEN-CENELEC/JTC 19 and EU Digital Identity Wallet Standards and Technical Specifications, "Technical Specification for Electronic Ledger Trust Services (CEN/TS 18264, Work in Progress)," Standards tracking documentation, 2025. https://github.com/eu-digital-identity-wallet/eudi-doc-standards-and-technical-specifications/issues/427

[33] International Telecommunication Union, "Electronic Ledgers in the eIDAS Regulation Revision," Workshop material, Feb. 20, 2023. https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2023/0220/Documents/Paolo%20Campegiani%202.pdf

[34] International Organization for Standardization, "ISO 23257:2022, Blockchain and Distributed Ledger Technologies - Reference Architecture," Standard, 2022. https://www.iso.org/standard/75093.html

[35] European Commission, European Blockchain Services Infrastructure, "EBSI Verifiable Credentials Framework" and "EBSI-VECTOR: Business Registries," 2026. https://ec.europa.eu/digital-building-blocks/sites/spaces/EBSI/pages/600343491/EBSI%2BVerifiable%2BCredentials ; https://ec.europa.eu/digital-building-blocks/sites/spaces/EBSI/pages/736755779/EBSI-VECTOR+Business+Registries

[36] World Economic Forum and Deloitte, "Transitioning to a Quantum-Secure Economy," White Paper, Sept. 13, 2022. https://www.weforum.org/publications/transitioning-to-a-quantum-secure-economy/

[37] World Economic Forum, "Innovation Ecosystems: A Toolkit of Principles and Best Practice," Report, Oct. 21, 2025. https://www.weforum.org/publications/innovation-ecosystems-a-toolkit-of-principles-and-best-practice/

[38] World Economic Forum, "Quantum Economy Network," Initiative, 2026. https://initiatives.weforum.org/quantum/home ; https://initiatives.weforum.org/quantum/application-hub

[39] M.-J. O. Saarinen, "Intro to Side-Channel Security of NIST PQC Standards," NIST PQC Seminar, Apr. 4, 2023. https://csrc.nist.gov/projects/post-quantum-cryptography/workshops-and-timeline/pqc-seminars