

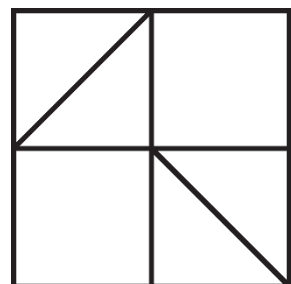
Magpie Projects

COLLECT . CONNECT . CREATE

Quantum-Safe Digital Assets & Crypto Agility: A strategic transformation blueprint for Bitcoin, Ethereum and Institutional Digital Asset Infrastructure

White Paper

September 2026



Executive summary

Digital assets prove ownership and authorise transfers using digital signatures. Cryptography is the asset, not a layer beneath it. No cryptographically relevant quantum computer exists today and significant engineering hurdles remain, but migration lead times for decentralised protocols and institutional custody estates run to years, and three developments in 2026 shortened the available planning window.

The cost estimates collapsed. In March 2026, Google Quantum AI, with the Ethereum Foundation, Berkeley and Stanford, put the 256-bit elliptic curve problem behind Bitcoin and Ethereum signatures at under 1,450 logical qubits and fewer than half a million physical superconducting qubits, an eighteen-fold reduction against the 2023 PsiQuantum benchmark. In September, IonQ published the first fully compiled end-to-end estimate for secp256k1: 19,397 physical qubits and 25.7 days per attempt, against prior trapped-ion estimates of 1.2 to 9.4 million. Both describe machines that do not exist today, but the direction of travel is unambiguous. The machine outlined could execute this attack in 2028, according to IonQ's roadmap, which is only 2 years from now.^{1,24}

What is at risk here is authenticity rather than secrecy. On a public ledger the data is already visible, so what matters is deriving a private key from an exposed public key and signing a valid transaction. That enables theft, validator impersonation, contract admin takeover and unauthorised movement of tokenised value. BlackRock's June assessment reaches a comparable conclusion: the binding constraint is coordination and execution rather than technology, and the advantage currently sits with the defence.¹⁷

For a German or EU-regulated institution the timetable is no longer abstract. The German Banking Industry Committee expects every institution to hold a cryptographic inventory by the end of 2027 and documented migration scenarios by the end of 2030, neither of which depends on a final protocol standard. The wider policy architecture hardened too: the G7 gave the financial sector its own six-phase migration model, and in August 2026 the US Treasury stood up a Quantum-Readiness Task Force with a digital assets workstream. Section 4 separates what is genuinely required from what is merely recommended. This paper applies Magpie's COLLECT . CONNECT . CREATE model to that work.^{3,12,13,14}

What changed in 2026

- The attack was quantified. At roughly nine minutes per key derivation, Bitcoin's ten-minute block time sits inside the on-spend window; Ethereum's twelve-second slots do not.¹
- A full attack blueprint appeared. In September, IonQ published a fully compiled end-to-end resource estimate for secp256k1: 19,397 physical qubits and 25.7 days per attempt, succeeding with 40.7 to 63.3 percent probability per attempt. Vendor-published, not peer reviewed.²⁴
- **Guidance started turning into obligation.** US Executive Order 14412 sets binding federal dates, key establishment by end-2030 and digital signatures by end-2031, plus a proposed contractor deadline. France's ANSSI gates product qualification on PQC from 2027.^{10,12}
- The financial sector got its own roadmap. The G7 Cyber Expert Group published a six-phase migration model in January, and on 24 August the US Treasury launched a Quantum-Readiness Task Force with a digital assets workstream.^{13,14}
- Germany put dates on it. GBIC expects a cryptographic inventory at every institution by end-2027; BSI's TR-02102-1 v2026-01 was the first version to carry migration deadlines, ending standalone classical key agreement at end-2031, end-2030 where protection needs are very high, and classical signatures at end-2035.^{3,21}
- The protocols published roadmaps. BIP-361 proposes a phased sunset of ECDSA and Schnorr spends, with roughly 35 percent of bitcoin supply having revealed a public key. The Ethereum Foundation dated seven L1 forks to 2029, five of them quantum-related.^{6,8,17}

Contents

Executive summary	2
1 Where the exposure actually sits	4
1.1 How close the hardware is	4
1.2 Three attack modes, three different clocks	4
2 Bitcoin and Ethereum are two different problems.....	6
3 The institutional control plane	7
4 What is required, what is recommended, what is advised.....	8
4.1 Group-level compliance: German entities inside US groups.....	9
4.2 Governance.....	10
Conclusion: why Magpie	11
A methodology for becoming crypto-agile	11
Where to start, and who owns what	11
How Magpie can help	12
Sources	13

1 Where the exposure actually sits

A blockchain transaction is an assertion of cryptographic control. Quantum risk enters wherever a public key, validator key or administrative key is both revealed and economically valuable. The binding constraint for institutions is rarely whether post-quantum cryptography exists. It is whether the surrounding estate of custody vendors, signing quorums, contract privileges and recovery paths can be migrated without fragmenting liquidity or breaking client access.

Where quantum risk sits in the digital asset stack

Market layer	Exchanges, ETPs, OTC desks, stablecoins, tokenised funds
Custody layer	HSM / MPC, hot and cold wallets, policy engines, recovery
Application layer	Smart contracts, bridges, L2s, oracles, admin multisigs
Ownership layer	Wallets, UTXOs, EOAs, transaction signatures, validator keys
Base protocol	Bitcoin L1 and Ethereum L1: consensus, data availability

Exposure concentrates wherever a public key, signing quorum or administrative control key is both revealed and economically valuable.

Figure 1: Where quantum risk sits in the digital asset stack

1.1 How close the hardware is

In September 2026, IonQ published the first fully compiled, end-to-end fault-tolerant resource estimate for Shor's algorithm applied to secp256k1, the elliptic curve underpinning Bitcoin and most digital asset signature schemes. The study puts the cost at 19,397 physical qubits and 25.7 days per attempt on a trapped-ion architecture using quantum LDPC codes, with a single attempt succeeding with probability between 40.7 and 63.3 percent depending on the postprocessing bound applied. Running five devices in parallel raises the probability that at least one succeeds to 99.3 percent without extending the elapsed time.²⁴

The significance is not the calendar date. It is the trajectory. Previous estimates for the same problem on trapped-ion hardware ranged from 1.2 million to 9.4 million physical qubits. The reduction comes from compiling every operation down to executable error-correction primitives rather than abstracting away the layers that dominate a real machine's runtime. Comparable estimates now exist for neutral-atom hardware at a similar or smaller scale, and a peer-reviewed 2023 result put the same problem at nine hours on roughly 126,000 cat qubits.²⁴

Three qualifications belong alongside the figure. The machine does not exist; the paper is an architectural study consistent with IonQ's stated roadmap for around 2028, published by a company with a commercial interest in the timeline, and it has not been peer reviewed. Part of the footprint reduction rests on a loss model the authors themselves describe as requiring further validation. And secp256k1 is a favourable target, because its pseudo-Mersenne prime admits optimisations that do not transfer directly to the NIST or brainpool curves used elsewhere in financial infrastructure.²⁴

For asset servicers the exposure is to authenticity and integrity rather than confidentiality. A signature compromise is exploitable forward in time, so it is not a store-now-decrypt-later problem and cannot be deprioritised on that basis. It is also the harder migration, because roots of trust, code signing and certificate hierarchies are the slowest components to replace. The standardised mitigations, ML-DSA and SLH-DSA, are unaffected by this class of attack, and BSI recommends the hedged variant of ML-DSA at NIST security strength categories 3 and 5.²¹

1.2 Three attack modes, three different clocks

Attack mode	What it targets	Why it matters to institutions
At-rest	Public keys already exposed on-chain or off-chain, attacked over days or longer.	Reused Bitcoin addresses, legacy P2PK and Taproot outputs, any Ethereum account that has ever transacted, dormant admin keys.

Attack mode	What it targets	Why it matters to institutions
On-spend	A public key revealed while a transaction waits for inclusion.	Bitcoin is in range: roughly 41 percent theft probability under idealised assumptions. Ethereum's twelve-second slots put it out of range for early fast-clock machines. ¹
On-setup	Fixed protocol parameters broken once, then exploited classically.	KZG commitments, pairing-based proof systems and some privacy protocols. Ethereum's KZG trusted setup holds if any one participant discarded their secret. ⁸

Table 1: Quantum attack modes and their institutional relevance

Proof-of-work is not the concern. Grover's algorithm gives only a quadratic speed-up against SHA-256, largely absorbed by error correction overhead and by Bitcoin's automatic difficulty adjustment. Both the Google and BlackRock analyses treat quantum mining as a non-issue.^{1,17}

2 Bitcoin and Ethereum are two different problems

Both depend on elliptic curve signatures, but they fail differently and migrate differently. Bitcoin has the narrower technical surface but the harder coordination problem. Ethereum has a dated roadmap and a far wider risk surface. Risk registers that carry a single line for digital asset quantum exposure will understate one of them.

	Bitcoin	Ethereum
Exposed value	Around 6.9 million BTC, roughly 35 percent of supply, is exposed to long-range attack: 1.9 million in script types that publish the key outright, plus about 5 million in hashed types that revealed keys through reuse. ^{17,19}	Around 20.5 million ETH in the top 1,000 accounts is exposed; a fast-clock machine could crack that set in under nine days. ¹
Concentration risk	Address reuse by exchanges and services; Taproot key-path spends reintroduced at-rest exposure. ¹	70 of the top 500 contracts hold about 2.5 million ETH behind admin keys, plus roughly 200 billion US dollars in stablecoins and tokenised RWAs. ¹
Consensus and data	Proof-of-work is not quantum-threatened. ^{1,17}	37 million ETH staked under BLS signatures; blob data availability under KZG commitments. ^{1,8}
Migration path	Soft fork. BIP-360 adds P2MR, Taproot without the vulnerable key path. BIP-361 proposes Phase A three years after activation, Phase B two years later. No consensus yet on scheme or timeline. ^{6,17}	Dated forks: Hegota in H2 2026 ships EIP-8141 native account abstraction; J* and I* in 2027 add PQ precompiles and a validator key registry; L* in 2028 adds leanXMSS attestations with leanVM aggregation; M* in 2029 moves blobs to STARK proofs. ^{8,17}
Unmigratable supply	Chainalysis estimates 2.3 to 3.7 million BTC, 11 to 19 percent of supply, may be permanently lost, including roughly 1.1 million in P2PK addresses widely attributed to Satoshi. ¹⁷	Dormant exposure is around 0.1 percent on EF estimates, which makes do-nothing far more viable. ^{7,8}
Binding constraint	Decentralised governance, plus the redistribution question over lost coins. Signature size also bites: SLH-DSA is roughly 7.8 KB, over 100 times a Schnorr signature. ¹⁷	Technical breadth: consensus, data layer, contracts, L2s and proof systems all migrate on different clocks.

Table 2: Comparative migration profile

The institutional read: map exposure by network rather than by ticker. A Bitcoin ETP, a staked ETH position and a tokenised fund on Ethereum sit on three different migration clocks with three different governance dependencies.

3 The institutional control plane

Most institutional loss would be operational before it is protocol-level: a compromised custody key, an exchange hot wallet, a bridge admin account, a stablecoin upgrade key. These systems combine on-chain signatures with off-chain HSMs, MPC networks, approval workflows and vendor software, so readiness has to be managed end to end rather than per chain.

Actor	Readiness focus	Primary constraint
Custodians	HSM and MPC roadmap, cold-wallet exposure, key rotation, recovery workflow, insurance evidence.	Vendor timelines and certification.
Exchanges	Hot-wallet minimisation, withdrawal batching, private order flow, client migration playbook.	Operational error during mass migration.
Stablecoin issuers	Mint, burn, freeze and upgrade keys; reserve-chain dependencies; chain-exit strategy.	Concentrated systemic control.
Tokenisation platforms	Fund admin keys, transfer-agent controls, contract upgrade rights, oracle dependencies.	Legal finality versus on-chain control.
Staking providers	Validator key exposure, slashing protection, client roadmap, PQ key registry readiness.	Consensus performance and service continuity.

Table 3: Where institutional readiness effort belongs

For German banks the perimeter is already mapped. GBIC names card-based payments and the ATM and POS estate, FinTS online banking, EBICS, the PSD2 certificate infrastructure and general secure internet communication as affected systems, and stresses that none of it moves without SWIFT, EMVCo, ECSG, EPC and the terminal, card and HSM manufacturers. Digital asset exposure sits on top of that estate.³

The first deliverable is a digital asset cryptographic bill of materials. It identifies every wallet, address type, public-key exposure state, signing quorum, vendor dependency, contract privilege, staking key, bridge dependency and recovery path, scored by asset value, exposure, migration friction and governance dependency. Public exposure registries such as Project Eleven's Bitcoin Risq List, used by both the Google and BlackRock analyses, can seed the Bitcoin side.^{1,17,19}

4 What is required, what is recommended, what is advised

The question institutions put to us is which of these dates a supervisor can actually hold them to. Today, little of it binds a European bank directly. The architecture hardened considerably during 2026 though, and guidance is steadily converting into obligation. The table below separates the three categories.

Anchor	Commitment and date	Status
GBIC (Die Deutsche Kreditwirtschaft)	Cryptographic inventory at every German banking institution by end-2027. Migration scenarios with prioritisation and fallbacks by end-2030. Crypto-agility by design in new applications. ³	Sector expectation rather than law, but the operative benchmark for German banks and the one a supervisor is most likely to reach for.
Germany (BSI)	TR-02102-1 v2026-01 ends its recommendation for standalone classical key agreement at end-2031, and at end-2030 for applications with very high protection needs. Classical signatures are expected to be recommended only to end-2035. Post-quantum methods should be deployed hybrid. ²¹	Technical guideline on algorithms and key lengths rather than a supervisory deadline for banks, but the reference document German auditors and evaluation bodies work from. Aligned with the EU roadmap on signatures, which the guideline states explicitly.
EU coordinated roadmap	National plans and pilots by end-2026. High-risk use cases by end-2030, with quantum-vulnerable public-key mechanisms not used stand-alone after that. Medium and low risk by end-2035. ²	Guidance to member states. Reaches institutions through national implementation.
France (ANSSI)	PQC obligations for entry into product qualification from 2027. Not reasonable to buy products without PQC after 2030. Hybrid required. ¹⁰	Binding inside the regulated perimeter, which covers classified and Diffusion Restreinte data, vital systems and product certification. Guidance outside it.
UK NCSC	Discovery by 2028, high-priority migration by 2031, complete by 2035. ⁴	Guidance. Benchmark for UK entities and shared infrastructure.
NIST	FIPS 203, 204 and 205 published 13 August 2024. NIST IR 8547 deprecates quantum-vulnerable algorithms and removes them by 2035, with high-risk systems much earlier. ^{5,11}	Binding for US federal systems. The de facto global algorithm baseline for everyone else.
US Executive Order 14412, 22 June 2026	Federal high-value and high-impact systems to PQC for key establishment by 31 December 2030 and for digital signatures by 31 December 2031. Proposed FAR rule to require covered contractors to meet PQC-incorporating FIPS by 31 December 2030. CISA and NIST to publish minimum elements for a cryptographic bill of materials. ¹²	Binding on US federal agencies. Reaches private firms through the federal contract chain.
G7 Cyber Expert Group, January 2026	2035 as the overall financial-sector target, with the most critical systems addressed in 2030 to 2032. Six-phase migration model. ¹⁴	Explicitly neither guidance nor regulatory expectation. The G7 CEG states this itself. Its value is as a shared vocabulary across jurisdictions.
US Treasury Quantum-Readiness Task Force, 24 August 2026	Public-private body with three workstreams: sector alignment and PQC transition, third-party and vendor readiness, and digital assets and emerging technology risk. ¹³	Voluntary, though it is the first G7 finance ministry structure with a named digital assets quantum workstream.

Table 4: Public authority anchors, separated by how binding they are

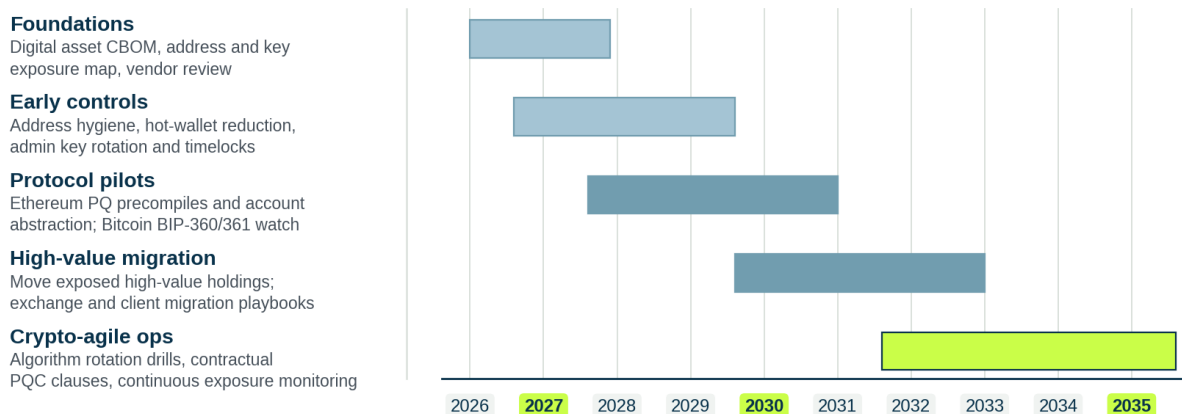
Two details belong in a board pack. First, the US executive order splits its deadlines: key establishment by end-2030, digital signatures by end-2031. Digital asset exposure is a signature problem, so it lands on the later and harder of the two, since post-quantum signatures are far larger than the ones they replace. BSI splits the same way with a wider gap: end-2031 for standalone classical key agreement against an expected end-2035 for classical signatures. So the German technical anchor for

signature exposure sits later than the surrounding table would suggest, which argues for pacing the case on custody and vendor readiness rather than on a supervisory clock.²¹ Second, that same order instructs CISA and NIST to publish minimum elements for a cryptographic bill of materials, which means the inventory this paper recommends is on its way to having a defined federal format. Institutions building one now should build it to be mappable rather than bespoke.¹²

European supervisors have converged on hybrid. ANSSI, BSI and GBIC all point to classical and post-quantum algorithms deployed together rather than post-quantum alone, and ANSSI makes hybrid mandatory inside its regulated perimeter, exempting only hash-based signatures. For vendor selection this means a supplier offering ML-KEM or ML-DSA on its own is not yet aligned with the European posture. Two caveats worth stating to clients: outside that regulated perimeter ANSSI's guidance carries no regulatory force today, and European certification does not itself mandate PQC.^{3,10,20,21}

Alongside the authorities, two private benchmarks matter. The Ethereum Foundation targets core post-quantum infrastructure around 2029, which sets the earliest credible date for PQ-native Ethereum custody. Google and Cloudflare both pulled their own migration deadlines forward to 2029 citing the March 2026 research, which is useful evidence that crypto-agility is deliverable and a reasonable bar to hold vendors to.^{7,8,9,17,18}

Institutional roadmap to crypto-agile digital asset operations



Highlighted years are external commitments, not Magpie estimates. 2027: GBIC cryptographic inventory at every German banking institution; ANSSI PQC obligation for product qualification. 2030: EU high-risk deadline; GBIC migration scenarios; BSI critical migration; ANSSI procurement line; US EO 14412 key establishment and federal contractors. 2035: EU, UK NCSC and G7 CEG full transition. Also: 2029 (Ethereum Foundation, Google, Cloudflare), 2030-32 (G7 CEG critical systems), 2031 (EO 14412 digital signatures), 2032 (BSI full).

Figure 2: Institutional roadmap to crypto-agile digital asset operations

4.1 Group-level compliance: German entities inside US groups

Many German institutions are subsidiaries, branches or joint-venture partners of US groups, or run US operations of their own. Group cryptographic policy, vendor framework contracts and internal audit standards are usually set centrally. In practice the US timetable reaches Frankfurt through the group, not through BaFin, and it often arrives earlier than the local one. Two channels matter. Where any group entity holds US federal business, the FAR rule proposed under Executive Order 14412 would require covered contractors to meet PQC-incorporating FIPS by 31 December 2030, and that obligation travels down through contract terms.¹² Where any part of the group serves National Security Systems, CNSA 2.0 applies to that part and tends to become the group algorithm baseline by default.¹⁵

CNSA 2.0 mandates ML-KEM and ML-DSA at Level V parameters for all classification levels, AES-256, SHA-384 or SHA-512, and LMS or XMSS for software and firmware signing. It states that this will effectively deprecate RSA, Diffie-Hellman, ECDH and ECDSA once mandated, expects transition complete by 2035, and sets exclusive use by 2030 for software and firmware signing and for networking equipment.¹⁵

Five practices stop a dual-jurisdiction programme splitting in two.

Make hybrid the group default. It is the highest common denominator. ANSSI requires it inside its regulated perimeter, BSI and GBIC point to it, and CNSA 2.0 explicitly permits hybrid where protocol standards, product availability or interoperability call for it, provided the post-quantum algorithm is present and selected. Hybrid is the one configuration needing no jurisdictional exception.^{3,10,15}

Standardise parameters upward, not downward. CNSA 2.0 requires Level V for all classification levels. A group setting ML-KEM-1024 and ML-DSA-87 as its floor clears the European bar too; a group standardising lower will need a carve-out for its US arm.¹⁵

Build one inventory, tagged for two schemas. GBIC wants an inventory at every German institution by end-2027, and CISA and NIST are defining minimum elements for a cryptographic bill of materials under the executive order. Build once and tag for both, so the German entity does not repeat discovery for group reporting.^{3,12}

Treat algorithm divergence as a board exception. CNSA 2.0's general-use suite is deliberately narrow, while ANSSI declines to publish a closed list and exempts hash-based signatures from its hybrid requirement. Where group policy and local supervisor diverge, that belongs on the board agenda with a documented rationale, since settling it quietly in configuration leaves no audit trail.^{10,15}

Read vendor validation claims precisely. CNSA 2.0 enforcement runs through NIAP validation and the Risk Management Framework, and states explicitly that National Security Systems should not be assessed against FIPS validation. European qualification runs through ANSSI-approved evaluation centres and BSI schemes. A vendor described as FIPS validated is not automatically acceptable in either regime, so ask which scheme, which scope and which date.^{10,15}

The planning rule follows from all five: align to the earliest binding date anywhere in the group rather than the local one. A German subsidiary inside a US group with federal contract exposure may face end-2030 through the contract chain, ahead of anything a German supervisor asks for, and well ahead of 2035. Plan to the earliest date and treat the later local deadlines as slack.

4.2 Governance

Prioritisation should be explicit: quantum risk multiplied by asset value, public-key exposure, migration friction and governance dependency. The highest scores are almost always hot wallets, exposed high-value UTXOs, contract admin keys, bridge controls, stablecoin privileges and custody vendors without a published PQC roadmap. The programme needs a named accountable executive, a protocol watch function, a custody owner, a vendor-risk owner and a crisis playbook for contested forks, and it should produce audit-grade evidence throughout. Dormant-asset policy cannot be solved internally and belongs on the governance register.

Conclusion: why Magpie

For an institution, quantum risk in digital assets shows up first as an ownership, custody and governance problem, and only then as a cryptography problem. Bitcoin and Ethereum can migrate. The institutional ecosystem around them cannot wait passively for protocol consensus, and the supervisors have now put dates on the work. What that calls for is a repeatable route to crypto-agility, meaning the ability to change a cryptographic algorithm in production without mounting a change programme each time. NIST makes the point plainly in its crypto-agility white paper, observing that this transition will certainly not be the last one required.²³

A methodology for becoming crypto-agile

The six steps below deliberately mirror the phase model in the G7 Cyber Expert Group roadmap, so an institution running this programme can map its progress directly onto the framework its supervisors and international counterparts are reading.¹⁴

- 1 Awareness and preparation (COLLECT).** Executive-level risk framing, a named accountable owner, and a first map of critical systems, sensitive data and the digital asset functions that depend on signatures.
- 2 Discovery and inventory (COLLECT).** A cryptographic bill of materials covering the digital asset estate and the banking systems it touches: wallets, address types, exposure state, signing quorums, contract privileges, staking keys, HSM and MPC dependencies, recovery paths and third parties. Build it to map onto the federal CBOM format now in preparation rather than to a bespoke schema.¹²
- 3 Risk assessment and planning (CONNECT).** Rank by value, exposure, migration friction and governance dependency, then split critical from non-critical work. The G7 model points critical systems at 2030 to 2032 and everything else at 2035. The output is a sequenced plan of work, and the technology choices follow from it.¹⁴
- 4 Migration execution (CONNECT).** Deploy progressively, priority functions first, hybrid by default. Test every vendor roadmap against the 2027 qualification gate and the 2030 procurement line, and run a standing protocol watch on Bitcoin and Ethereum.
- 5 Migration testing (CREATE).** Measure latency, signature size, throughput and recovery on real paths, and rehearse at ecosystem level so the case rests on the institution's own measurements rather than on a vendor claim.
- 6 Validation and monitoring (CREATE).** Algorithm rotation as a rehearsed drill, PQC clauses in contracts, continuous exposure monitoring, and quantum risk carried in the standing risk framework rather than a one-off programme.

Three things run continuously alongside all six: embedding quantum-resistant cryptography into existing governance and risk management, active management of external dependencies including vendor and standards maturity, and structured stakeholder dialogue across the sector. These are the G7 CEG's own continuous lines of effort, and they are the parts most easily deferred once delivery pressure builds.¹⁴

Where to start, and who owns what

Most institutions stall on this because it has no natural owner. It reads as a cryptography problem, so it lands with engineering, where it competes with delivery. The work below is split by role so that each owner can act without waiting for the others.

Who	What you own	First deliverable	The date that binds you
Board and executive directors	The funded decision and the documented position.	A minuted board position on quantum risk, with a named accountable executive.	The 2026 or 2027 budget cycle, since GBIC expects the inventory complete by end-2027. ³
Technology and information security	The inventory and the migration sequence.	A cryptographic bill of materials covering the digital asset estate and the banking systems it connects to.	End-2027. Group deadlines from a US parent may fall earlier. ^{3,12}
Digital assets and business lines	Exposure inside the products you sell.	An address and key exposure map per product, plus your custody vendor's written position.	Before signing any new custody, ETP or tokenisation mandate.

Who	What you own	First deliverable	The date that binds you
Risk and compliance	The evidence and the supervisory narrative.	Quantum risk on the register, and PQC readiness folded into the cryptographic policy and certificate register you already maintain.	Now. The DORA technical standards already require you to update cryptographic technology as cryptanalysis develops. ¹⁶
Procurement and vendor management	Contract terms.	PQC and crypto-agility clauses in every new contract and every renewal from this quarter onward.	ANSSI gates product qualification from 2027; the proposed FAR rule reaches contractors by end-2030. ^{10,12}
Third-party and technology providers	Your own roadmap, published.	A dated PQC roadmap naming algorithms, parameter levels and hybrid support, written so a client can attach it to a due diligence file.	Your bank clients will ask during 2027 procurement rounds. ^{10,13}

Table 5: First actions by role

For compliance officers there is a shortcut worth knowing. The DORA technical standards do not mention post-quantum cryptography, and nobody should claim otherwise. But Commission Delegated Regulation 2024/1774 already requires financial entities to hold an encryption and cryptographic controls policy with provisions for updating cryptographic technology on the basis of developments in cryptanalysis, and to maintain a register of certificates and certificate-storing devices for assets supporting critical or important functions. Those obligations are live today. Much of the machinery this paper calls for can be built inside them rather than alongside them, which is usually the difference between a funded control enhancement and an unfunded new programme.¹⁶

The cost of waiting is asymmetric. Starting now is inexpensive, because the inventory takes weeks and depends on no protocol decision that has yet to be made. Starting in 2029 means running discovery, vendor renegotiation, migration and testing at the same time, against fixed dates, in a market where every comparable institution is bidding for the same scarce specialists. The sequencing advantage is available once.

How Magpie can help

We frame the business and supervisory case, set the target operating model, build the governance and board reporting, and hold vendors and delivery to account. The cryptographic implementation work, meaning key management engineering, HSM and library integration and cryptographic testing, runs through specialist partners under our programme governance. The separation is deliberate. It keeps your advisor independent of the technology being selected, which matters most when the algorithm choice is contested. Three engagements cover the first phase.

Exposure baseline, four to six weeks. A cryptographic bill of materials for the digital asset estate and connected banking systems, a scored exposure heatmap, a vendor gap list, and a summary written for the board rather than for engineering.

Supervisory readiness review, three to four weeks. Your current position mapped against GBIC end-2027, the EU end-2030 threshold, BSI end-2031 for classical key agreement and end-2035 for classical signatures, and any group deadlines inherited from a US parent, with the documented rationale internal audit and supervisors will ask to see.

Programme design and assurance, ongoing. Operating model, governance and board reporting, vendor negotiation support, and delivery assurance across the six phases set out above.

If the decision is not yet ready to be made, the exposure baseline is the smallest step that produces something a board can act on. It answers the only two questions that matter at this stage: how much of what we hold is exposed, and which of our vendors cannot yet tell us their plan. Contact details are on the final page.

Sources

Primary and official sources

1. Babbush, Zalcman, Gidney et al., Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities: Resource Estimates and Mitigations. Google Quantum AI with the Ethereum Foundation, UC Berkeley and Stanford. arXiv:2603.28846, submitted 30 March 2026, revised 15 April 2026. Also IACR ePrint 2026/625. <https://arxiv.org/abs/2603.28846>
2. European Commission and NIS Cooperation Group, A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, 23 June 2025. digital-strategy.ec.europa.eu
3. Die Deutsche Kreditwirtschaft (German Banking Industry Committee), Position Paper on the Impact of the Development of Quantum Computers, 05/2025. Supplied as PDF; no public URL verified at time of writing.
4. UK NCSC, Timelines for migration to post-quantum cryptography. <https://www.ncsc.gov.uk/guidance/pqc-migration-timelines>
5. NIST CSRC, Post-Quantum Cryptography Standardization. csrc.nist.gov/projects/post-quantum-cryptography
6. BIP-361, Post Quantum Migration and Legacy Signature Sunset, draft, assigned 11 February 2026. github.com/bitcoin/bips
7. Ethereum Foundation Post-Quantum team, pq.ethereum.org, last updated 27 June 2026. <https://pq.ethereum.org/>
8. ethereum.org, Post-quantum cryptography on Ethereum, roadmap page, updated 12 July 2026. ethereum.org/roadmap/security/quantum-resistance
9. Google Cloud, Post-quantum cryptography resource hub and 2029 migration roadmap. cloud.google.com/security/resources
10. ANSSI (France), FAQ sur la cryptographie post-quantique. States the 2027 qualification obligation, the 2030 procurement position and the hybrid requirement. cyber.gouv.fr/enjeux-technologiques/cryptographie-post-quantique
11. NIST IR 8547, Transition to Post-Quantum Cryptography Standards. Sets the deprecation and removal timeline referenced by NIST's PQC project page. csrc.nist.gov/pubs/ir/8547/ipd
12. Executive Order 14412, Securing the Nation Against Advanced Cryptographic Attacks, 22 June 2026. whitehouse.gov/presidential-actions/2026/06
13. U.S. Department of the Treasury, Treasury Announces the Quantum-Readiness Task Force, 24 August 2026. home.treasury.gov/news/press-releases/sb0615
14. G7 Cyber Expert Group, Advancing a Coordinated Roadmap for the Transition to Post-Quantum Cryptography in the Financial Sector, January 2026. home.treasury.gov/system/files/136/G7-CEG-Quantum-Roadmap.pdf
15. NSA, Announcing the Commercial National Security Algorithm Suite 2.0, cybersecurity advisory PP-22-1338. media.defense.gov/CSA_CNSA_2.0_ALGORITHMS.PDF
16. Commission Delegated Regulation (EU) 2024/1774 of 13 March 2024 (DORA technical standards on ICT risk management). Article 6 covers encryption and cryptographic controls, Article 7 cryptographic key management and the certificate register. eur-lex.europa.eu/eli/reg_del/2024/1774/oj
21. BSI, Technische Richtlinie TR-02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 2026-01, 23 January 2026. bsi.bund.de
22. BIP-360, Pay to Quantum Resistant Hash (P2QRH / P2MR), draft. github.com/bitcoin/bips
23. NIST CSWP 39, Considerations for Achieving Crypto Agility: Strategies and Practices, 19 December 2025 (upd1 as of 29 June 2026). doi.org/10.6028/NIST.CSWP.39
24. Häner, Tripiër, Young, Naehrig, Maksymov, Alam, Maslov, Parrott, de Sereville, Sullivan, Webster, Delfosse, Gamble and Roetteler (IonQ Inc.), Computing 256-bit elliptic curve discrete logarithms in 26 days on a fault-tolerant trapped-ion quantum computer with 20,000 qubits, 3 September 2026, published 8 September 2026, 70 pp. Vendor-published and not peer reviewed; to be cited as a resource estimate, never as an established result. cdn.prod.website-files.com (PDF); investors.ionq.com (announcement)

Industry and vendor sources

17. BlackRock, Quantum Computing and Blockchains, June 2026 (ref. GPS0626-5553059-EXP0627). Authors: Will Su, Inish Crisson, Robert Mitchnick. blackrock.com/us/financial-professionals/insights
18. Cloudflare, Post-quantum cryptography. Vendor primary for its own network deployment. <https://www.cloudflare.com/pqc/>
19. Project Eleven, Bitcoin Risq List. Commercial vendor; the exposure registry used by sources 1 and 17. projecteleven.com
20. PostQuantum.com (Marin Ivezić), France's ANSSI Will Block PQC-Free Products From Certification Starting 2027, 17 June 2026. Expert commentary; the underlying announcement was reported by Reuters, 16 June 2026. postquantum.com/security-pqc/anssi-pqc-certification-2027

Authors



Niklas Hegemann

Industry Partner

Telefon +49 157 806 230 46

niklas.hegemann@magpieprojects.com

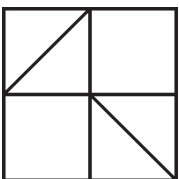


Christian Behm

Partner

Telefon +49 172 6207111

christian.behm@magpieprojects.com



Emerging from LPA Consulting, we bring over two decades of capital markets expertise but now sharpen our focus on forward-looking strategic transformation.

We act on early insights to help clients stay ahead, transforming intelligence into actionable strategies and guiding clients from traditional capital markets toward the more integrated financial markets, where public and private capital flows intersect.

We stay at the forefront of change, helping clients navigate shifts—whether in policy, technology, or changing structures. We ground ambition in experience, enabling faster decisions and measurable outcomes. As financial markets evolve, so must the tools. We embed AI and use your data to build smarter, scalable systems, always applying technology with purpose.