eBook

THALES
CYBERSECURITY

The Quantum-Safe Financial Enterprise

A Thales blueprint for operationalizing crypto-agility, reducing HNDL exposure, and producing audit-ready evidence by 2030.

cpl.thalesgroup.com

Contents

How to use this eBook

This guide is designed for CISOs, security engineering leaders, PKI and identity teams, network and infrastructure owners, operational resilience teams, and risk/audit stakeholders who need a defensible plan and proof for PQC transition. Many organizations are now moving beyond initial cryptographic discovery and proof-of-concept efforts toward establishing full governance of cryptographic infrastructure, with defined ownership, lifecycle management, and continuous validation.

This is a practical, strategic guide. Use it to align stakeholders and move from intent to measurable progress.

- Define what "ready by 2030" means in terms your governance and auditors can validate.
- Stand up a two-track program that reduces exposure now while longer migrations proceed.
- Set short-term deliverables (first 60–90 days) that establish control and validate the path through a contained pilot, rather than attempting to complete the full enterprise migration.

How to read it

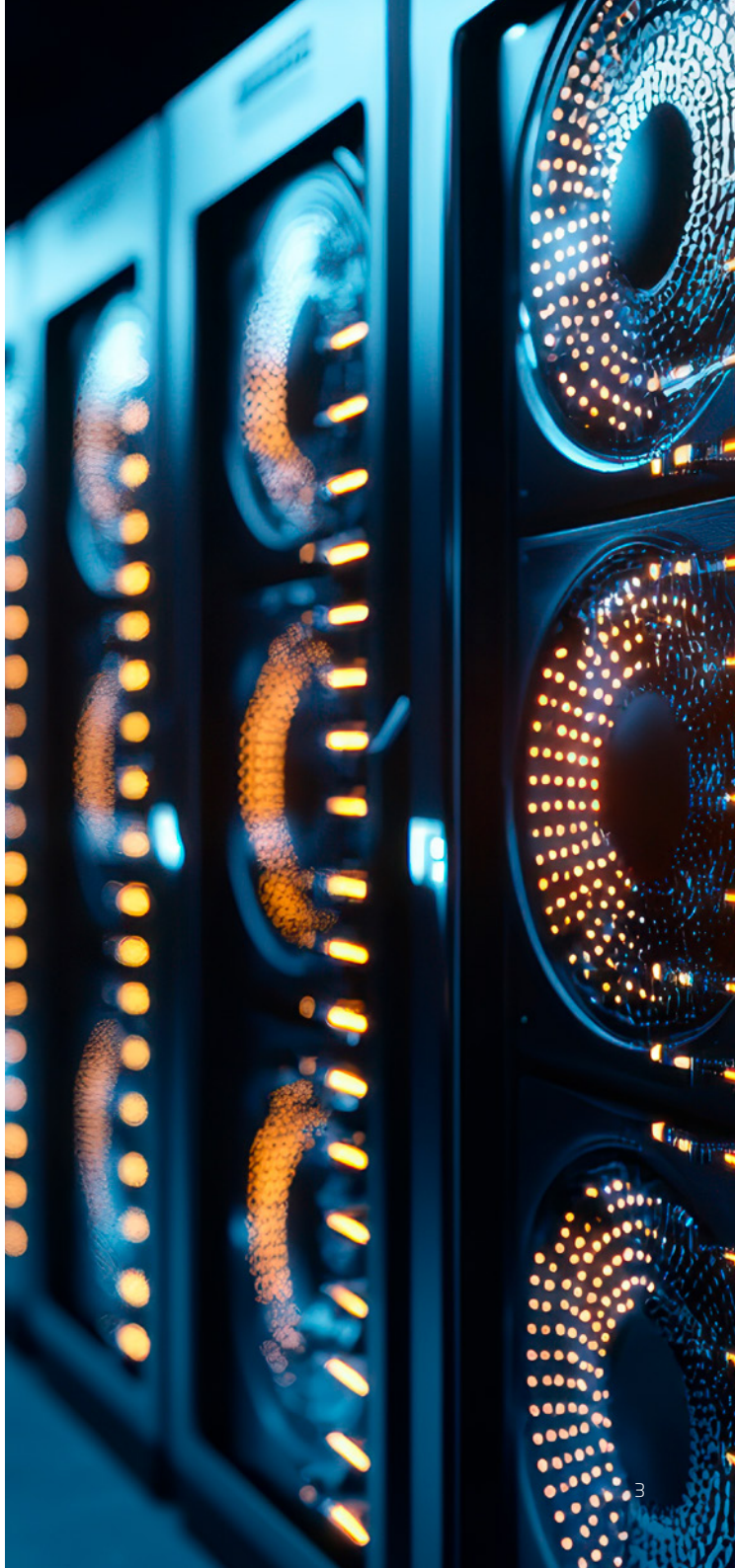
Use it in three passes:

1. Executive alignment: agree what "ready by 2030" means and what evidence will be required.
2. Program design: stand up the two parallel workstreams and assign ownership.
3. Action: deliver a contained pilot and produce evidence as part of delivery, not after the fact.

What to copy into your program artifacts

As you read, capture three living registers:

- Crypto system of record (where cryptography is used, ownership, constraints)
- Interoperability register (external dependencies and readiness gates)
- Evidence pack index (what proof you maintain continuously)



Executive Summary

Crypto-agility is not just a configuration setting; it spans protocols, applications, libraries, hardware, firmware, and the operational processes that connect them. Designing for agility lets you adopt new algorithms and retire vulnerable ones without disrupting operations.

2030 is not the moment to begin your post-quantum cryptography (PQC) journey. It is the point by which cryptographic resilience must be demonstrably in place. For financial services institutions (FSIs), PQC readiness is a multi-year engineering and operational program with long dependency chains and a high bar for evidence, control, and resilience.

Emerging industry guidance is already shifting expectations earlier, with some projections indicating readiness targets closer to 2029, further compressing timelines for discovery, testing, and migration.

Harvest now, decrypt later (HNDL) is a present-day risk: adversaries can capture encrypted data today with the intent to decrypt it later once cryptographically relevant quantum computing becomes viable, exposing years or decades of sensitive information. In parallel, organizations must also consider emerging risks such as harvest now, forge later (HNFL), where future capabilities could be used to compromise the integrity of digital signatures and trust chains.

Waiting for ecosystem readiness compresses discovery, testing, supplier coordination, and operational change into an unsafe window.

Start now. Build your crypto inventory and test harnesses, engage suppliers early, capture evidence as you go, and migrate in phases aligned to risk and readiness.

Best-practice guidance from NIST and industry supports running two parallel tracks from day one:

Track 1

Protection for data, identities, transactions, and critical applications.

Standardize how cryptography is consumed, anchor key custody and signing in HSM-rooted trust, and build crypto-agility into documented, repeatable change packages so upgrades are safe, measurable, and reversible.

Track 2

Data-in-motion protection for critical interconnects you control.

Reduce HNDL exposure immediately by securing the network paths you control with high-assurance, transport-flexible encryption that avoids forcing changes to the underlying network design.

In practice, these two tracks are commonly anchored by HSM-based trust for keys and signing—such as Thales Luna HSMs—and by high-assurance link encryption on critical network routes, such as Thales High Speed Encryptors network encryption solutions.

What ready by 2030 means

"Ready by 2030" is measurable. It means you can demonstrate control, execute cryptographic change safely, and produce evidence continuously across defined scope and ownership.

01

You can show where cryptography is used, who owns it, and what the change constraints are through a maintained crypto system of record.

02

You have tested and recorded PQC impacts in representative environments, including performance, interoperability, and operational procedures.

03

You can introduce new cryptographic profiles in controlled phases using documented, repeatable change packages, including test plans, rollout and recovery procedures, monitoring, incident handling, and high-availability and disaster-recovery validation.

04

You are migrating in controlled phases, starting where you control both ends, with clear gate criteria for cutovers to external ecosystems such as third-party partners, payment rails, market infrastructure, SaaS providers, cloud-managed services, customer clients and browsers, devices, and cross-border affiliates.

05

You maintain audit-ready evidence continuously, rather than treating it as a one-time documentation exercise.

Why financial services institutions must act now

Program risk comes first.

Quantum risk often shows up first as program risk: not knowing where cryptography is used, who owns it, what systems are hard to upgrade, and how to change safely under examiner scrutiny. When discovery starts late, FSIs lose the option to sequence calmly and prove outcomes.

Operational pressure is already increasing as certificate lifecycles tighten. The CA/Browser Forum Baseline Requirements include a published schedule that reduces maximum public TLS certificate validity over time (for example, to 200 days for certificates issued on or after March 15, 2026; to 100 days on or after March 15, 2027; and to 47 days on or after March 15, 2029). This increases renewal volume and makes ownership, automation, and change control part of resilience, not just hygiene.

Long confidentiality horizons create urgency

Financial services data frequently carries confidentiality horizons measured in years to decades. If protected information is captured today and later decrypted, the impact can extend beyond immediate fraud. It can create reputational harm, affect market integrity, increase regulatory exposure, and introduce competitive risk. This urgency is reinforced by accelerating progress in cryptographically relevant quantum computing (CRQC) and the well-established impact of Shor's algorithm, which directly targets widely used public-key cryptography. Industry analyses continue to highlight the risk of earlier-than-expected disruption.

Practical implication

- Start discovery early to avoid unknowns.
- Build a test environment and record facts (performance, interoperability, operational impact).
- Reduce exposure quickly on links you control while application modernization proceeds.

Standards and transition reality: what to plan around

The safest migration approach is to anchor plans to standardized algorithms and to design for change as profiles mature. NIST has standardized an initial set of PQC algorithms, and adoption will roll out unevenly across platforms, products, and third parties.

In practice, organizations must be able to introduce new profiles, retire exposed algorithms, and manage interoperability shifts without disruption.

Crypto-agility is a business requirement.

NIST post-quantum cryptography standards

01

Role: **Key establishment**

Standard: **FIPS 203**

NIST FIPS 203 standardizes ML-KEM for establishing shared keys, a common building block for TLS and other secure channels.

02

Role: **Digital signatures**

Standard: **FIPS 204**

NIST FIPS 204 standardizes ML-DSA as a primary post-quantum signature standard used across signing and PKI workflows.

03

Role: **Alternate signature option**

Standard: **FIPS 205**

NIST FIPS 205 standardizes SLH-DSA as a stateless hash-based signature option used for some assurance and deployment profiles.

What standardization means for your migration

01

Prioritize the right use cases. Start with controlled trust paths and links you can execute and prove, where you control both endpoints and the operating model, while mapping and testing ecosystem-dependent paths in parallel. Use the interoperability register to gate cutovers as partners and providers become ready. Prioritization should also be data-centric, with cryptographic upgrades aligned to data classification, confidentiality horizons, and business criticality. This ensures that the highest-risk assets are addressed first rather than applying uniform migration approaches across all systems

02

Plan for hybrid operation. Many ecosystems are likely to support hybrid approaches before PQC-only deployments are practical. Hybrid operation can provide a workable transition path, but it introduces additional complexity, larger handshakes, and more interoperability and testing overhead. Use it deliberately: validate it thoroughly, protect negotiation against downgrades, define policy dates for retiring legacy algorithms, and treat hybrid as a transitional state with explicit exit gates rather than a permanent end state.

03

Define scope boundaries early. Be explicit about what is in scope for Phase 1 (for example, TLS, IPsec/MACsec, SSH, PKI, code signing, and data-at-rest) and what is deliberately out of scope until later phases.

04

State assumptions and dependencies. Call out target platforms (on-prem, cloud, SaaS), third-party constraints, and where hybrid (classical + PQC) is expected as an interim state so delivery plans and evidence expectations match reality.

05

Test operational impact. Larger certificates and different handshake characteristics can affect load balancers, proxies, and termination points. Measure baselines and deltas in a representative lab.

06

Treat validation as readiness. Build an evidence pack that includes algorithm support status, test results, and operational runbooks. In regulated environments, align assurance artifacts to your governance needs, for example, FIPS validation and Common Criteria where applicable.

Track updates.

Maintain an interoperability register and monitor NIST's PQC standardization project for updates.

Emerging guidance such as NIST CSWP 39 reinforces this approach, outlining how organizations should establish cryptographic governance as an ongoing capability, including inventory, policy enforcement, lifecycle management, and continuous validation.

For additional transition guidance, see NIST IR 8547, "Transition to Post-Quantum Cryptography Standards."

Track 1: Protection for data, identities, transactions, and critical applications

Anchor cryptographic operations in an HSM-rooted trust model to support high-assurance key protection, signing services, and PKI processes. Where centralized governance across environments is required, some institutions complement HSM-based controls with centralized key management, policy, and audit visibility across hybrid and multi-cloud estates.

A common gap in FSIs is that encryption and key controls often grow organically by line of business. Each area may meet local requirements, but the enterprise still lacks a complete, owned view of where cryptography is used, what dependencies exist, and how changes can be made safely under governance.

Where Thales fits: FSIs often use Thales Luna HSMs as the hardware root of trust for PKI and signing services, with controlled upgrade paths as standards and profiles evolve. To extend that control across hybrid and multi-cloud environments, teams commonly layer in the Thales CipherTrust Data Security Platform (CDSP) for centralized key management, policy, and audit visibility across applications and data stores, while keeping sensitive keys protected by HSMs where required. CDSP can also help organizations prioritize effort by focusing on higher-risk data sets and the cryptographic dependencies that protect them.

In practice, a crypto system of record stays defensible only if it stays current. That is why institutions pair governance with cryptographic discovery and inventory processes that can identify keys, certificates, crypto libraries, ciphers, and trust paths across live environments. The operating model matters as much as the technology: ownership, validation, refresh cadence, and exception handling all need to be defined.

Make ownership explicit: assign accountable roles for PKI, application teams, network encryption, vulnerability management, and audit evidence production, including the refresh cadence for inventories, test results, and runbooks.

Practical starting points:

- Identify trust anchors (internal PKI, issuing CAs, signing services, key ceremony processes) and map them into the crypto system of record.
- Pick one Phase 1 internal use case for PQC and hybrid testing, such as internal service-to-service TLS or an internal signing workflow.
- Standardize how applications consume crypto services to reduce one-off implementations and accelerate upgrades.

In practice, good looks like this:

- Applications consume standardized crypto services, not bespoke implementations.
- Keys and signing are anchored in governed trust services with clear ownership.
- Cryptographic changes move through documented, reversible change packages.

Track 2: Data-in-motion protection for critical interconnects you control

Reduce near-term HNDL exposure by encrypting critical links you control, including inter-site, inter-data center, and cloud connectivity such as data center-to-cloud, cloud-to-cloud, and connections to key external providers where both endpoints and the operating model are under your control.

In Track 2, "control" means you can deploy and operate encryption end to end without waiting for application changes or third-party upgrades. This often includes links you operate directly: inter-site, inter-data center, cloud, backup, disaster recovery, and selected partner connectivity where responsibilities are clearly defined.

Where Thales fits: Thales High Speed Encryptors (HSE) are widely used to protect high-value networks where teams need predictable performance at scale, high availability, and straightforward operational control. In a PQC transition, they also provide a practical platform for proving real-world crypto-agility on critical routes: validating complete cryptographic profiles (not just one algorithm) and deploying protection quickly without forcing application changes or redesigning the underlying network.

For Track 2, validate the full cryptographic profile that will operate in production—not just individual algorithms. Where certificate-based negotiation is appropriate, test PQC (or hybrid PQC/classical) key establishment together with your intended authentication model and certificate profile. Validate the associated KDF used to derive session keys, as well as the symmetric encryption and integrity algorithms that ultimately protect traffic in motion. Confirm session management, monitoring, failover, and change procedures end to end.

Where a certificate-less mode is preferred, confirm that endpoints can operate without any on-wire key exchange by deriving successive AES session keys from a securely provisioned root derivation key using a standard KDF. Verify rekey cadence, replay protection, monitoring signals, and downgrade or rollback protections. Validate how that model affects provisioning, rollover, recovery, auditability, and separation of duties.

Hybrid operation often provides a practical bridge during transition because it preserves classical security while adding PQC resistance and supporting interoperability as endpoints and providers mature. It should still be treated as a transitional state with explicit exit criteria, not a permanent destination.

A practical differentiator evaluated in this track is Transport Independent Mode (TIM), used by Thales High Speed Encryptors. TIM enables tunnel-free encryption across Layers 2, 3, and 4, helping teams protect diverse transports—including cloud connectivity—without forcing a network redesign. This makes it easier to add protection quickly on critical routes while maintaining operational predictability and performance.

What to validate in the first pilot (Track 2):

- Baseline performance: Measure throughput and latency under load and define acceptance criteria for scaling.
- Operational predictability: Prove failover behavior, maintenance workflow, monitoring signals, and key rollover runbooks.
- Assurance alignment: Confirm your assurance posture matches procurement and audit expectations (for example, reliance on validated modules and independent assurance such as FIPS validation and Common Criteria where applicable).
- Document TIM fit: Identify routes or environments where tunnel-free encryption simplifies deployment and avoids the need for routing changes or network redesign.

Since TIM can operate without on-wire key exchange by deriving session keys from a securely provisioned root derivation key using a standard KDF, it can also reduce the harvest-now, decrypt-later exposure associated with capturing negotiation traffic for future decryption attempts. This makes Track 2 the fastest path to measurable HNDL exposure reduction.

Three moves that create momentum (and reduce risk fast)

If you do only three things early, start here. They reduce uncertainty quickly and create momentum that auditors and governance teams can follow.

When building a crypto system of record, teams often pair governance with cryptographic discovery to populate the inventory of keys, certificates, crypto libraries, ciphers, and trust paths from live environments. This improves coverage and helps keep the inventory current, but it still requires ownership, validation, and exception handling to remain defensible.

Many organizations are now moving beyond initial discovery and proof-of-concept efforts toward full governance of cryptographic infrastructure, with defined ownership, lifecycle management, and continuous validation. Industry approaches similarly emphasize building and maintaining a comprehensive cryptographic inventory as a foundation for ongoing posture management and risk reduction.

01

Stand up a crypto system of record with ownership and measurable scope coverage.

02

Build an interoperability register and use it to gate external cutovers.

03

Define an evidence pack and produce it continuously as part of delivery.

What to produce now and keep updated

> Treat these as living artifacts that support governance, planning, and audit-ready evidence throughout the migration program.

01

Crypto system of record:

Systems and services, owners, crypto usage, protocols and profiles, key lifecycles, confidentiality horizon, and change constraints.

02

Interoperability register:

External dependencies, readiness status, blockers, test evidence, and target phase.

03

Evidence pack index:

A structured index of evidence artifacts, including test results, validation records, operational runbooks, and change documentation maintained continuously throughout the program.

Short term (first 60–90 days): establish control and prove the path

Timelines vary by institution size and complexity. Here, "short term" refers to the first 60–90 days. The goal is to establish discovery, validate impacts in a representative lab, and complete a controlled pilot where you control both ends.

Days 0 to 30	Actions
Create the crypto system of record with ownership, dependencies, and confidentiality horizons. Practical starting point: begin with server certificates and trust paths (where certificates terminate and how they are issued).	
Stand up the interoperability register for top external dependencies (partners, browsers and clients, SaaS, devices).	
Define evidence artifacts to produce continuously (inventory metrics, test results, runbooks, change records).	
Identify hard-to-upgrade systems and define compensating controls.	

Days 31 to 60	Actions
Build a representative PQC test environment and record results.	
Measure performance and operational impacts (handshake latency, certificate sizes, infrastructure constraints).	
Validate rollback and high-availability behaviors for critical cryptographic services and protected links.	
Test hybrid approaches where partner and platform readiness is uneven.	

Days 61 to 90	Actions
Deploy a controlled pilot where you control both ends (one critical link and one Phase 1 internal trust path).	
Document operational runbooks for failover, maintenance, monitoring signals, and key rollover.	
Convert lab outcomes into a repeatable reference implementation.	
Define Phase 2 and Phase 3 gating criteria based on interoperability readiness and operational confidence.	

Phased model: migrate without a big bang

The phased model keeps delivery controlled and measurable, and it aligns naturally with what you can control and what you can prove.

01

Phase 1:

Internal trust paths and controlled inter-site links where you control both ends.

02

Phase 2:

High-value regulated assets, including long-term archives, backups, and privileged paths.

03

Phase 3:

External-facing ecosystems and partner APIs, gated by interoperability readiness and test evidence.

To keep phases measurable (and defensible under scrutiny), define clear metrics and gates: coverage targets for the crypto system of record, required test cases, cutover criteria, and the minimum evidence artifacts expected at each phase.

Plan for exceptions up front: maintain a register for hard-to-upgrade systems, document compensating controls, and set policy dates for retiring legacy algorithms as platforms and partners become capable.

Common gate criteria for Phase 3:

- Partners and client platforms have stated support, and you have test evidence.
- Operational procedures are validated, including rollback, monitoring, incident handling, and high availability and disaster recovery.
- Evidence pack artifacts are produced and accepted by internal audit or risk governance.

Regulatory and supervisory signals

Most regulators are not prescribing specific post-quantum algorithms yet. What they are doing globally is raising the bar on operational resilience, third-party risk discipline, and demonstrable control, as reflected in the references below. A disciplined PQC program aligns well with that direction because it requires inventory, testing, governance, evidence, and controlled change.

AMER

01 Canada. OSFI Guideline B-13 on Technology and Cyber Risk Management.
www.osfi-bsif.gc.ca

02 US. FFIEC IT Examination Handbook booklet on Architecture, Infrastructure, and Operations (AIO).
www.occ.gov

03 Considerations for Achieving Cryptographic Agility: Strategies and Practices. NIST Cybersecurity White Paper, NIST CSWP 39.
nvlpubs.nist.gov

EMEA

01 EU. Digital Operational Resilience Act (DORA), Regulation (EU) 2022/2554.
eur-lex.europa.eu

02 UK. FCA PS21/3 on building operational resilience.
www.fca.org.uk

APJ

01 Australia. APRA CPS 230 Operational Risk Management.
www.apra.gov.au

02 Hong Kong. HKMA Cybersecurity Fortification Initiative (CFI) and C-RAF.
www.hkma.gov.hk

03 Singapore. Advisory On Addressing The Cybersecurity Risks Associated With Quantum
www.mas.gov.sg

Global references

01 Basel Committee Principles for operational resilience.
www.bis.org

02 CPMI-IOSCO cyber resilience guidance for financial market infrastructures (ECB overview).
www.ecb.europa.eu

Takeaway: across regions, the supervisory direction is consistent. Demonstrable control, tested resilience, and disciplined third-party risk management matter.

Next steps:
launch your PQC program

If you want to move from planning to measurable progress, start with a focused working session and a controlled pilot.

01

Book a PQC readiness working session with Thales to align on scope, priorities, and Phase 1 migration candidates.

02

Define your crypto system of record, interoperability register, and evidence-pack templates.

03

Build a lab validation plan that produces facts on performance, interoperability, and operational impact.

04

Select a controlled pilot for one critical link and one internal trust path.

Ready by 2030 is measurable, and it starts now. Thales can help financial institutions launch a two-track PQC program that reduces HNDL exposure on critical links today while building the controls, visibility, and evidence needed for longer-term application, PKI, and ecosystem migrations. Start with a focused working session, establish your crypto system of record and interoperability register, and execute a controlled pilot where you control both ends.

Contact Thales to operationalize crypto-agility and PQC readiness across both tracks so you can reduce exposure now and demonstrate audit-ready progress through 2030.

About Thales

Thales is a global leader in cybersecurity, helping businesses, governments, and the most trusted organizations in the world protect critical applications, sensitive data, identities, and software anywhere, at scale — with the highest ROI. With more than 30,000 customers, including 58% of the Fortune Global 500, our solutions are deployed in 148 countries around the world. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

THALES

CYBERSECURITY

Contact us

For contact information, please visit cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com