ETSI/IQC Quantum Safe Cryptography Conference 2026

Cryptographic Agility: An Enterprise Operating Standard

Presented by:

Leila Taghizadeh

Global Head of Cyber Risk Management, Allianz

Co-Authors: Jelena Zelenovic, Edoardo Pena-Gonzalez, Jaime Gómez Garciía, Bart Preneel | COSIC, KU Leuven, Leuven, Belgium

18/06/2026

OPENING: THE RIGHT QUESTION

✗ **The Wrong Question**

When will a cryptographically relevant quantum computer arrive?

This frames cryptographic risk as a future event, something to respond to when it arrives.

Most PQC programmes are stuck here.

✓ **The Right Question**

Can you change your cryptography when you need to, without breaking your business?

This frames cryptographic agility as an organisational capability, one that must be built before pressure arrives.

PQC is not the point. It is the stress test.

Roadmap to quantum resilience where we stand and what comes next

2025 – 2026
OpenSSL 3.5 & major browsers support PQC by default

~2031
NIST partial deprecation of vulnerable cryptography

~2033 – 2035
NIST declares vulnerable crypto obsolete — full disallowance

GOVERNMENT DEADLINES

Australia
Plan: 2025
Implement: 2025
Stop vulnerable: 2031

Canada
Plan and implement: : 2025
Stop vulnerable: 2035

EU
Plan: 2025
Implement: 2026
Stop vulnerable: 2035+

India (Proposal)
Plan: 2026
Implement: 2028
Stop vulnerable: 2033

UK
Plan and implement: 2027
Stop vulnerable: 2035

US
Plan: 2025
Implement: 2026
Stop vulnerable: 2032

FINANCIAL SECTOR DEADLINES

Bank of Israel
Plan: 2026
Implement: 2026
Type: Recommendations

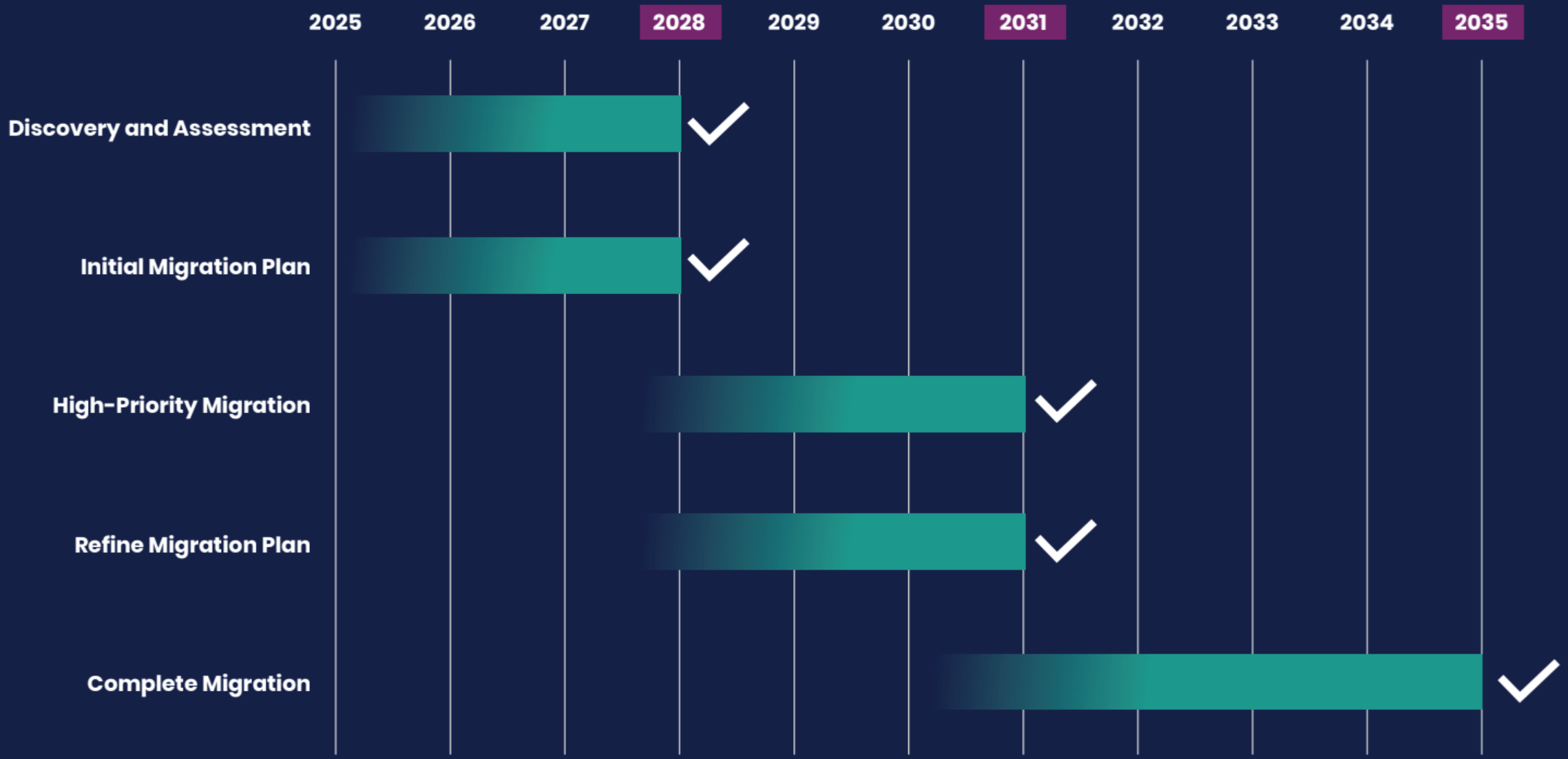
M.A. Singapore
Plan: 2026
Type: Recommendations

India (SEBI)
Plan: 2025
Implement: 2028
Stop vulnerable: 2033

G7 CEG
Plan: 2025
Implement: 2025
Stop vulnerable: 2035

National Cyber Security Centre
a part of GCHQ

PQC Migration Timeline



Mosca's Inequality flags what is already exposed - Treat PQC as a governed capability, not a project

Trust lifetime (X) + Migration time (Y) > Quantum threat horizon (Z)

If this inequality holds for any asset, that asset is already exposed — regardless of when a quantum computer arrives.

X Trust lifetime

How long must this data or signature remain secure?

- KYC records: 10+ years
- Signed contracts: 30 - 50 years
- Regulatory filings: 7 - 10 years
- Insurance policies: lifetime

Most critical financial assets have X > 10 years.

+

Y Migration time

How long will migration take?

- TLS: months
- PKI re-issuance: 1 - 3 years
- HSM replacement: 3 - 7 years

Most organizations underestimate Y by 2–3×.

>

Z Quantum threat horizon

When will a CRQC be available?

- Global Risk Institute 2024: 2025
- NIST deprecated RSA: 2030
- NIST disallows RSA: 2035
- EU Commission critical target: 2030

Z is uncertain. That uncertainty is the risk.

PQC Migration is a multi-layer program, including no-regret actions!

Layer 1: Network & Transport Controls

Layer 2: Trust Infrastructure

Layer 3: Identity & Authentication

Layer 4: Data & Long-Lived Assets

Layer 5: Hardware & Root of Trust

Layer 1: Network & Transport Controls

CIPHER SUITE COMPONENTS BY PROTOCOL VERSION

Component	SSL 3.0 DISABLE NOW	TLS 1.0 DISABLE	TLS 1.1 DISABLE	TLS 1.2 HARDEN & SUNSET	TLS 1.3 ENFORCE
Key Exchange	RSA key transport Non DH (no auth) Export-grade 40-bit NO FWD SECRECY	RSA transport [X] DH static [X] DHE / ECDHE (ok) Export-grade [X]	Same as TLS 1.0 RSA transport [X] DH static [X] DHE / ECDHE (ok)	UNSAFE: RSA [X] DH static [X] Export-grade [X] SAFE: DHE / ECDHE All coexist - config risk	ECDHE / DHE only Ephemeral mandatory Forward secrecy enforced + ML-KEM (PQC hybrid)
Authentication	RSA / Anonymous [X] No cert validation in SSLv2 suites	RSA / DSA / ECDSA Anonymous [X] Identity unverifiable	RSA / DSA / ECDSA Anonymous [X] Same risk as TLS 1.0	UNSAFE: Anonymous [X] DSA deprecated [X] SAFE: RSA / ECDSA Config discipline needed	RSA-PSS / ECDSA EdDSA / ML-DSA (PQC) Anonymous removed DSA removed
Encryption Cipher	RC4 / RC2 / DES 3DES / IDEA All broken - no AEAD Padding oracle risk	RC4 [X] / DES [X] 3DES [X] / AES-CBC [X] No AEAD at all BEAST attack on CBC	RC4 [X] / DES [X] 3DES [X] / AES-CBC [X] BEAST partially patched POODLE still applies	UNSAFE: RC4 DES 3DES [X] AES-CBC [X] (POODLE) SAFE: AES-GCM ChaCha20-Poly1305	AES-128-GCM AES-256-GCM ChaCha20-Poly1305 AEAD only - all safe
Hash / Integrity	MD5 only [X] Collisions trivial No SHA support	MD5 [X] / SHA-1 [X] Both broken Collisions demonstrated	MD5 [X] / SHA-1 [X] Both broken Same as TLS 1.0	UNSAFE: MD5 [X] SHA-1 [X] SAFE: SHA-256 SHA-384 / SHA-512 All coexist - config risk	SHA-256 / SHA-384 SHA-512 MD5 & SHA-1 removed All safe

[X] BROKEN disable immediately [!] WEAK harden config, set sunset deadline [OK] SAFE enforce as minimum

ACTION:

Scann (using e.g. Qualys, Tenable) all TLS versions and cipher suites in use across services.
Hard-disable SSL & TLS 1.0/1.1, Harden TLS 1.2: restrict to ECDHE+AEAD only, set sunset deadline
Enforce TLS 1.3 as minimum for all new services
Pilot ML-KEM hybrid (X25519MLKEM768) on critical services

Layer 2: Trust Infrastructure

Certificate Category · Types Covered	ML-DSA Standard	Available Now	HNDL Risk	Migration Complexity
① **PKI FOUNDATION** · Root CA · Intermediate CA · OCSP Signing · Timestamps (TSA)	YES	PARTIAL	YES	VERY HIGH
② **NETWORK & TRANSPORT** · TLS Server Certificates · VPN Gateway & RADIUS	PARTIAL	PARTIAL	YES	HIGH
③ **IDENTITY & ACCESS** · Client & Machine Auth · Domain Controller (LDAPS / PKINIT) · SAML / Federation Signing	PARTIAL	PARTIAL	PARTIAL	HIGH
④ **SIGNING & INTEGRITY** · Code Signing · Document Signing · S/MIME Email	PARTIAL	NO	YES	MED-HIGH
⑤ **EMBEDDED & CONSTRAINED** · IoT Devices · Industrial & OT Systems · Medical & Embedded	PARTIAL	NO	YES	VERY HIGH

Migrate in order ①→⑤ · Root CA unblocks every category · PARTIAL = pilot / internal CA only · HNDL risk spans 4 of 5 categories

Layer 3: Identity & Authentication

Action	Do Now?	Complexity	Risk if Delayed
Inventory all auth mechanisms SSH keys, FIDO2 tokens, JWT keys, machine certs, Kerberos PKINIT, SAML — map every surface	YES	LOW	VERY HIGH
Discover non-human identities Service accounts outnumber human accounts 5–10×; largely undiscovered and unmigrated	YES	MEDIUM	VERY HIGH
SSH: transport now / key type later ML-KEM key exchange: OpenSSH 9.0+ now (L1 action) · ML-DSA host/user key type: inventory now, execute later	PARTIAL	MEDIUM	HIGH
Rotate OAuth / OIDC JWT signing keys Blocked: python-jose, nimbus-jose-jwt lack ML-DSA support · Inventory keys and test experimental builds	NOT YET	HIGH	HIGH
Replace FIDO2 hardware tokens No PQC-capable FIDO2 hardware exists · Define procurement specs, monitor YubiKey / HID / Google roadmaps	NOT YET	VERY HIGH	HIGH
Migrate SAML federation to OIDC SAML has no PQC standard and will not get one — migration is independent of PQC, start now	YES	HIGH	MEDIUM
Audit PAM tools CyberArk, BeyondTrust, Delinea manage highest-privilege credentials; routinely missed in discovery	YES	LOW	VERY HIGH

Do now: items 1, 2, 6, 7 · Partial: SSH transport via Layer 1 now; ML-DSA key type later · Items 4 & 5: plan now, execute when ecosystem ships

Layer 4: Data & Long-Lived Assets

Action	Do Now?	Complexity	Risk if Delayed
Classify data by confidentiality duration Apply Mosca Inequality: retention + migration time > threat horizon = act now. Drives all other actions in this layer	YES	MEDIUM	VERY HIGH
Map RSA key hierarchies AES-256 data is quantum-safe. The RSA/ECDH key wrapping it is not. Find every RSA-wrapped key store and backup key	YES	HIGH	VERY HIGH
Re-encrypt high-value archives (hybrid) On-prem HSM pilot or AWS/Azure KMS preview: begin now for critical data · Full-scale production: partial, tooling constraints	PARTIAL	VERY HIGH	VERY HIGH
Re-sign long-lived documents with LTV Blocked: ETSI PAdES PQC profile not published; PQC CA certs not commercially available · Embed LTV (OCSP+TSA) in all docs signed today	NOT YET	HIGH	HIGH
Audit backup encryption Identifying RSA-wrapped backup master keys is free today · Re-keying follows when backup vendor PQC support ships	YES	MEDIUM	HIGH
Migrate cloud and on-prem KMS Cloud KMS preview environments available now for testing · On-prem blocked on Layer 5 HSM firmware availability	PARTIAL	HIGH	VERY HIGH
Establish data classification programme Mandatory prerequisite before re-encryption can be prioritised — without classification, migration is guesswork	YES	MEDIUM	HIGH

AES-256 is quantum-safe, the RSA key wrapping it is not
HNDL is active today: adversaries may already hold captured ciphertext

Layer 5: Hardware & Root of Trust

Action	Do Now?	Complexity	Risk if Delayed
Audit HSMs for PQC firmware availability Thales Luna, Utimaco, Entrust nShield — firmware may update; some devices require hardware replacement	YES	MEDIUM	VERY HIGH
Plan and schedule HSM key ceremonies now Quorum of cardholders, physical presence, notarisation — months to organise per cluster; cannot be compressed	YES	HIGH	VERY HIGH
Audit TPM inventory by version TPM 1.2: no upgrade path, hardware replacement required · TPM 2.0: vendor-dependent firmware support	YES	MEDIUM	HIGH
Plan smart card replacement programme No firmware upgrade for secure elements; physical replacement · Engineering samples available; production 2025–26	PARTIAL	VERY HIGH	HIGH
Assess BIOS/UEFI secure boot migration Risk: incorrect execution renders devices unbootable · Some tooling available now; test on isolated fleet first	PARTIAL	HIGH	HIGH
IoT/OT gateway proxies + procurement policy PQC TLS proxies for non-upgradeable devices: deploy now · PQC hardware clause in all new contracts: enforce today	YES	HIGH	VERY HIGH
Confirm FIPS 140-3 ML-DSA status with vendors FIPS 204 published Aug 2024; HSM FIPS 140-3 certification typically 12–24 months after standard · Query vendors now	YES	LOW	HIGH

Runs in parallel with all layers
Plan key ceremonies before firmware arrives, waiting costs are 6–12 months

What Does an Operating Standard Mean?

✓ In Scope

- How cryptographic use cases are identified across the enterprise
- How agility is assessed per use case using evidence-based criteria
- How remediation is prioritised proportional to trust lifetime
- How governance evidence is produced for audit and oversight

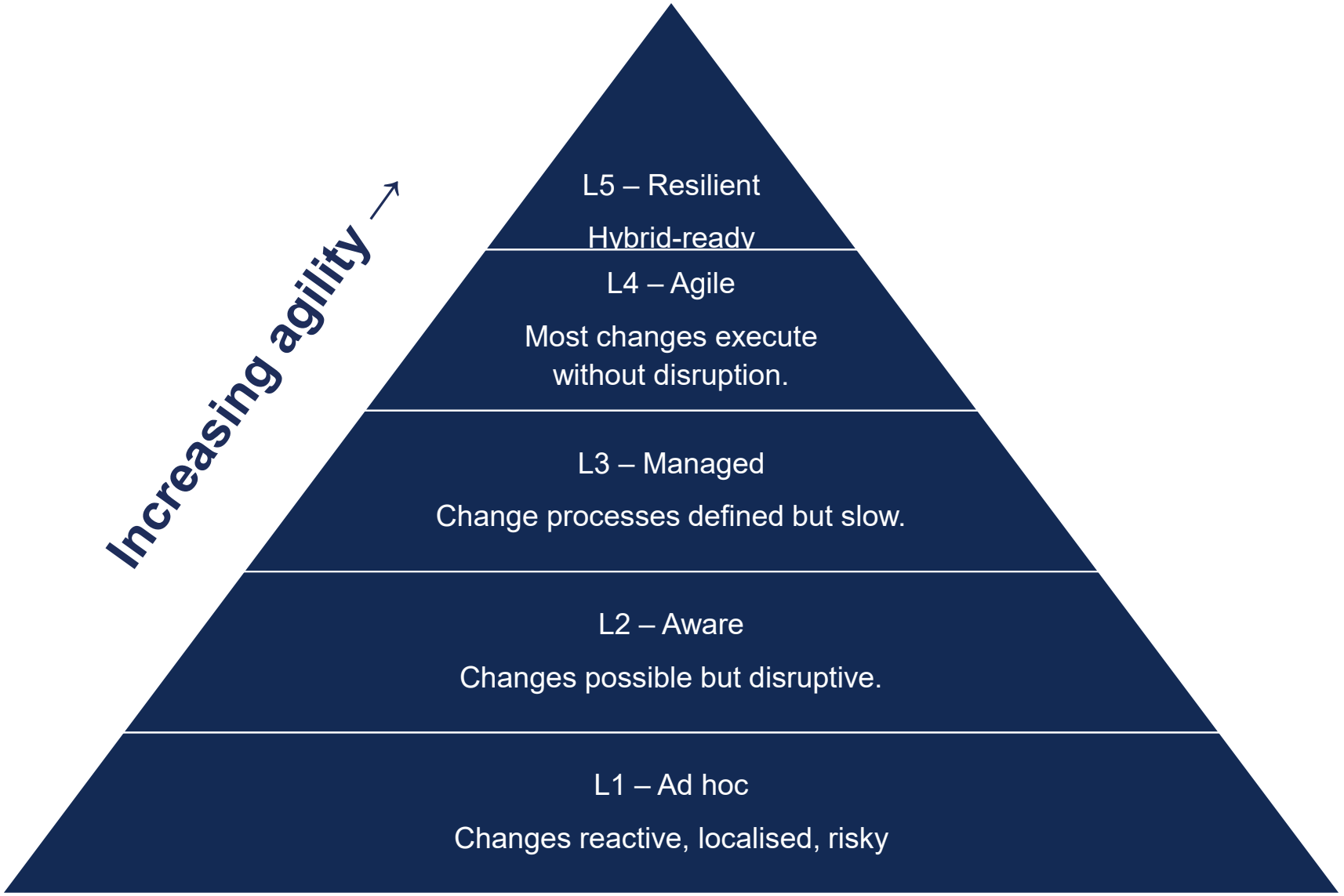
✗ Not In Scope

- Evaluating cryptographic algorithm strength
- Assessing implementation correctness or code security
- Prescribing which algorithms to use
- Formally ratified cryptographic standard or compliance obligation

⊙ Unit of Assessment

- The cryptographic USE CASE — not the organisation as a whole
- Each use case scored on 7 observable dimensions
- Required agility scales with trust lifetime (not a fixed bar)
- Evidence from configs, contracts, change records — not interviews

Cryptographic Agility Maturity Model



Evidence-Based Assessment: 7 Dimensions

	LOW	MED	HIGH
1. Network & Transport Controls Cipher suite negotiation, TLS enforcement, protocol agility across all paths	1	2	3
2. Trust Infrastructure Certificate lifetimes, trust anchor decoupling from applications and legal artefacts	1	2	3
3. Identity & Authentication Algorithm agility in HSM hardware, certification timelines, lifecycle procedures	1	2	3
4. Data & Long-Lived Assets Archive re-encryption capability, key wrapping metadata, backup key management	1	2	3
5. Application Design & Code Coupling Hardcoded algorithms, abstraction layers, code coupling to cryptographic primitives	1	2	3
6. Vendor & Third-Party Dependencies Vendor roadmap commitments, contractual upgrade rights, PQC timelines	1	2	3
7. Governance, Process & Evidence Cryptographic change lifecycle, cadence of reassessment, board-level oversight	1	2	3

Assessments are evidence-based: config exports, PKI audit logs, vendor contracts, architecture diagrams, change records. Absence of evidence scores Low.

Validation Case: Life Insurance Policy Signing

Business

Life insurance — regulated financial services

Infrastructure

Hybrid on-premises / cloud

Regulatory Context

Insurance regulation, data protection law, financial audit requirements

Trust Lifetime

30 to 50 years (policy lifetime)

Selected Use Case: Digital signing of life insurance policies at issuance to ensure authenticity, integrity, and non-repudiation over the contract lifetime.

Cryptographic Landscape

- Central enterprise PKI operated by a managed service provider
- HSM-backed signing keys for policy issuance
- Mix of legacy applications and modern service-oriented platforms
- Long-term document archives stored in encrypted form

Required Agility

= 3.0

Long-lived trust — all 7 dimensions must score High

Assessment Results: Observed vs. Required (Required 3.0)

Dimension	Score	Required	Gap
1. Network & Transport Controls Cipher suite negotiation, TLS enforcement, protocol agility across all paths	2	3	-1
2. Trust Infrastructure Certificate lifetimes, trust anchor decoupling from applications and legal artefacts	1	3	-2
3. Identity & Authentication Algorithm agility in HSM hardware, certification timelines, lifecycle procedures	2	3	-1
4. Data & Long-Lived Assets Archive re-encryption capability, key wrapping metadata, backup key management	1	3	-2
5. Application Design & Code Coupling Hardcoded algorithms, abstraction layers, code coupling to cryptographic primitives	1	3	-2
6. Vendor & Third-Party Dependencies Vendor roadmap commitments, contractual upgrade rights, PQC timelines	2	3	-1
7. Governance, Process & Evidence Cryptographic change lifecycle, cadence of reassessment, board-level oversight	2	3	-1
Aggregate	1.57	3.0	-1.43

This migration is structurally different – Treat PQC as a governed capability, not a project

Data Confidentiality Risk

Long-lived data scales with trust lifetime. A 5-year file may be acceptable risk; a 30-year insurance contract is already exposed.

Certificate and Identity Risk

A harvested CA private key does not reveal old data. It forges future identity — certificates, code signatures, infrastructure impersonation — undetected and indefinitely.

Migration is no longer a one-off event

- 3DES to AES and SHA-1 to SHA-2 transitions were bounded, **painful, but finite**.
- The endpoint explosion has changed the equation permanently. Within APIs, microservices, containers, IoT and edge, the cryptographic attack surface has grown 10–100× since the last major migration.

AI + quantum shorten the replacement cycle

- **AI accelerates cryptanalysis,** independently of quantum hardware. This means the interval between **cryptographic migrations will shorten.**
- Lattice-based ML-KEM and ML-DSA underpin the NIST 2024 standards. As quantum hardware scales, lattice hardness assumptions may themselves come under pressure.

Do we know how much cryptography we own?

- 40 - 60% of cryptographic use in large enterprises is **undocumented**. Third-party platforms, FMIs, cloud providers, and SaaS carry cryptographic dependencies that cannot be seen or migrated unilaterally.
- Crypto agility is not just about what we own. It is about **knowing precisely where our boundaries end and our ecosystem begins**.

THANK YOU!