PAREK Framework – EU Post-Quantum Cryptography Transition Handbook

2025-07-02

Contents

1 1 Document Control & Revision History

This file provides the authoritative revision history for the *PAREK Framework – EU Post-Quantum Cryptography Transition Handbook*. Update **only** via pull-request. Each entry must be approved by the Handbook Steering Committee.

Version	Date (YYYY-MM-DD)	Editor	Section(s) changed	Change description
0.1	2025-06-24	PAREK Editorial Team	Initial skeleton	Created document control template

1.0.1 How to update

1. Increment the **version** number using semantic format (e.g., `0.2`, `1.0`).
2. Add a concise **change description** (100 characters).
3. If multiple sections change, list comma-separated values in **Section(s) changed)**.
4. Commit the file and open a pull request tagged `#document-control`.

2 2 Executive Summary

> **Purpose of this section** – provide senior stakeholders with a concise, non-technical overview of the quantum-threat context, the PAREK Framework's objectives, and the high-level roadmap that underpins the handbook. This one-pager should be intelligible to board members, regulators and project sponsors.

2.1 Executive Summary (draft placeholder – to be expanded in v0.2)

The advent of **cryptographically-relevant quantum computers (CRQC)** will render today's RSA and ECC protections ineffective, putting long-lived confidential data at risk of *harvest-now-decrypt-later* attacks. To safeguard digital sovereignty and comply with forthcoming EU mandates, organisations must transition to **post-quantum cryptography (PQC)** well before widely available CRQC capabilities emerge.

The **PAREK Framework** offers a five-stage lifecycle—**P**ost-quantum asset & algorithm inventory, **A**ssessment of quantum risk, **R**oad-mapping & readiness

planning, **E**xecution & migration, and **K**ey-governance & continuous improvement. It aligns with the EU Coordinated Implementation Roadmap timelines (inventory baseline by 2026, high-risk cut-over by 2030, and medium-risk completion by 2035) and integrates NIST FIPS-validated algorithms (ML-KEM, ML-DSA, SPHINCS+).

Successful adoption hinges on three pillars: 1. **Comprehensive discovery** of cryptographic assets (CBOMs) across the entire estate. 2. **Risk-based prioritisation** using the Quantum-Adjusted Risk Score (QARS). 3. **Supplier integration** via contract clauses and machine-readable attestations.

By following PAREK, the organisation will achieve crypto-agility, maintain regulatory compliance, and preserve stakeholder trust in the quantum era.

(This text is a high-level placeholder. Subsequent revisions will incorporate quantitative risk metrics, budget highlights and KPI snapshots once sections 8–15 are finalised.)

3 3 Purpose, Scope & Audience

> **Purpose of this section** – clarify *why* the handbook exists, *what* systems and data it covers, and *who* should read and apply its guidance.

3.1 3.1 Purpose (placeholder)

The *PAREK Framework Handbook* establishes a common, evidence-based approach for migrating the organisation's cryptography to post-quantum algorithms in alignment with EU regulatory timelines and industry best practice. It consolidates policies, processes and technical playbooks into a single authoritative source.

3.2 3.2 Scope (placeholder)

> *To be detailed in v0.2 once the asset inventory (§8) and risk classification (§9) are baselined.*

Domain	In scope?	Notes (draft)
Production apps		All customer-facing and back-office apps

Domain	In scope?	Notes (draft)
Dev/test envs		CI/CD pipelines, test data masks
OT/ICS networks		Pending risk assessment outcome
Third-party SaaS		Subject to CBOM/contract clauses (see §13)
Legacy mainframe		Migration feasibility under investigation

3.3 3.3 Audience (placeholder)

Primary readers: - **Executive sponsors** (CIO, CISO, CRO) – governance & budget - **Security architects / cryptographers** – technical standards - **Product & dev-ops teams** – implementation guidance - **Procurement & legal** – supplier clauses, contract annexes - **Regulators & auditors** – compliance evidence

Secondary readers: - Vendors, open-source maintainers, academic reviewers.

> Subsequent revisions will flesh out scope exclusions, detailed audience personas, and cross-references to internal policies once sections 4–15 mature.

4 4 Regulatory & Strategic Context

> **Purpose of this section** – highlight the EU directives, national regulations and international standards that drive the organisation's post-quantum transition, and explain how the PAREK Framework aligns with these external obligations.

4.1 4.1 EU regulatory landscape *(placeholder)*

- **NIS 2 Directive** – security and reporting duties for essential/important entities.

- **Cyber Resilience Act (CRA)** – forthcoming product-security requirements incl. cryptographic transparency.

- **EU Coordinated Implementation Roadmap for PQC (2025)** – joint milestones: inventory 2026, high-risk cut-over 2030, medium-risk 2035.

(Detailed mapping to be added when national transposition timelines are confirmed.)

4.2 4.2 Strategic alignment *(placeholder)*

Describe how the organisation's cyber-security strategy, data-classification policy and digital-sovereignty goals intersect with PQC adoption.

4.3 4.3 External standards map *(placeholder)*

Standard	Status	Relevance to PAREK
NIST FIPS 203-205	Final	Baseline algorithms (ML-KEM, ML-DSA, SPHINCS+)
ISO/IEC DIS 14888-4	Draft	PQ signatures
ETSI TS 103 829	Stable	Hybrid key exchange

(Will expand once draft texts are ratified.)

Subsequent revisions will add jurisdiction-specific compliance deadlines, cross-reference to §15 KPIs, and commentary on industry guidance (e.g., ENISA reports).

5 5 Quantum Threat Landscape

Purpose of this chapter – present an evidence-based assessment of how, when and why quantum computing threatens today's cryptographic defences, and establish the urgency that underpins every subsequent stage of the PAREK Framework.

5.1 5.1 Executive overview

A new generation of **cryptographically-relevant quantum computers (CRQC)** threatens to break RSA and elliptic-curve public-key cryptography,

as well as reduce the effective security of some symmetric systems. Although no public demonstration of large-scale key-recovery exists as of *June 2025*, the physics, engineering and economic trends analysed in this chapter indicate that organisations must complete the transition to post-quantum cryptography (PQC) **well before 2035** to avert the twin risks of *harvest-now-decrypt-later* (HNDL) attacks and regulatory sanction.

Key messages:

- Commercial hardware roadmaps (IBM "Kookaburra" 1,386-qubit chip, planned for late 2025) illustrate a **quadratic growth curve** comparable to early classical Moore's Law (ibm.com).
- Expert-elicitation studies (Global Risk Institute *Quantum Threat Timeline 2024 & 2025*) put the median arrival of a CRQC capable of breaking RSA-2048 in the **early-to-mid 2030s**, with a 10 % probability the event occurs **before 2030** (globalriskinstitute.org, globalriskinstitute.org).
- Real-world HNDL behaviour is now documented across sectors such as maritime logistics and financial services (marinelink.com, keyfactor.com).
- Regulators have moved from guidance to **mandatory timelines** (e.g., US OMB M-23-02, EU Coordinated Implementation Roadmap, Europol Quantum Safe Financial Forum) (reuters.com).

The remainder of this chapter unpacks these trends and quantifies the residual uncertainty.

5.2 5.2 From laboratory curiosity to CRQC

A CRQC is not just a bigger quantum processor; it must combine **millions of physical qubits**, fast classical co-processing and robust error correction to implement Shor's algorithm at scale. The consensus path involves:

1. **Hardware scaling** – IBM's 1,121-qubit *Condor* (2024) and planned 4,158-qubit multi-chip Kookaburra system (2025-26) (ibm.com, ibm.com).
2. **Error-correction breakthroughs** – low-overhead surface codes + lattice surgery lowering logical-to-physical ratios by 30-50 % (published Nature, Feb 2025).
3. **Interconnects & parallelism** – photonic links to cluster cryostats, already demonstrated in AWS Braket prototypes.

Resource-estimation papers (Gidney & Ekerå 2023) suggest breaking RSA-2048 would require ~20 M physical qubits running for 8 hours at 10−3 physical error rates. The delta between current prototypes and this target is shrinking annually by **1-2 orders of magnitude**.

5.3 5.3 Threat timeline projections

5.3.1 5.3.1 Survey-based forecasts

The Global Risk Institute's *2024 Quantum Threat Timeline* surveyed 61 experts across academia and industry. Results (Figure 1) assign:

- 10 % probability of CRQC by **2029**
- 50 % probability by **2033-2035**
- 90 % probability by **2039-2040**

An updated *2025 Executive Perspective* report, focusing on financial-sector CISOs, reveals that **one-third of respondents shortened their internal "must-migrate-by" date by 2 years** compared with 2023 (globalriskinstitute.org).

5.3.2 5.3.2 Engineering trend extrapolation

IBM's roadmap shows qubit count doubling roughly every 18 months since 2017. If sustained, a 2-M qubit device (roughly RSA-2048 breaking threshold) is plausible by **2031-2033**. While *hardware alone is not destiny*, software stack and cryogenics must co-evolve; yet venture-capital funding ballooned to USD 4.2 B in 2024, signalling market capacity to close those gaps.

5.4 5.4 Harvest-now-decrypt-later evidence

Analysts at Keyfactor and Mandiant observe APT groups stockpiling TLS-encrypted session captures and VPN archives since at least 2021. Shipping-sector telemetry from Marlink (Q4 2024) logged nine billion encrypted packets exfiltrated and stored in off-net buckets (keyfactor.com, marinelink.com). Although current classical resources cannot decrypt them, **data confidentiality lifetimes**—especially in finance, healthcare and national security—often exceed 25 years, bridging the gap to plausible CRQC dates.

5.5 5.5 Regulatory accelerants

Jurisdiction	Mandate	Deadline
United States	OMB M-23-02: agencies submit PQC inventory → migrate high-impact systems	Inventory 2027; migration end-2035
European Union	Coordinated Roadmap: inventory baseline, high-risk cut-over	2026; 2030; 2035
Brazil	Central Bank circular on quantum-safe data storage	2032
Global finance	Europol-backed Quantum Safe Financial Forum urges "prepare now"	Guidance Feb 2025 (reuters.com)

NIST cemented the algorithm baseline with **FIPS 203 (ML-KEM), 204 (ML-DSA) and 205 (SPHINCS+)** in August 2024, removing a key blocker to production rollout (csrc.nist.gov).

5.6 5.6 Sector-specific impact analysis

5.6.1 5.6.1 Finance

- Long data retention (KYC, trade archives) + high Target Value (TV) migration priority.
- Real-time performance constraints encourage **hybrid TLS 1.3 (Kyber+ECDHE)** as interim measure.

5.6.2 5.6.2 Healthcare

- Patient records need 70-year confidentiality.

- Medical devices often lack firmware update paths → hardware refresh cycles must accelerate.

5.6.3 5.6.3 Critical infrastructure

- Industrial control protocols (OPC UA, DNP3) historically weak on crypto; retrofit costs high.
- Quantum risk intersects safety risk → regulator scrutiny rising.

5.7 5.7 Risk quantification models

5.7.1 5.7.1 Mosca inequality

`T_shelf-life + T_migration > T_threat` `exposure` * `T_shelf-life` – required confidentiality window (years) * `T_migration` – time to complete PQC rollout (years) * `T_threat` – forecast years until CRQC

Applying median GRI threat horizon (2034) and typical bank migration estimate (7 years) leaves organisations with **< 2 years to start** if they store 10-year confidential data.

5.7.2 5.7.2 Quantum-adjusted risk score (QARS)

Section 9 formalises QARS = `w · (T_shelf/T_threat) + …`. This chapter seeds baseline values for `T_threat` according to expert surveys, and Section 9 will refine per sector.

5.8 5.8 Emerging technical counter-measures

1. **Hybrid key exchange** – IETF RFC 9399 profiles Kyber + X25519.
2. **Hash-based signatures** – SPHINCS+ for firmware where statelessness matters.
3. **Quantum-resistant VPNs** – WireGuard fork with Kyber prime, early pilots at European research networks.
4. **Hardware crypto-agility** – HSM vendors announcing firmware roadmaps targeting FIPS 203 Level 3 by 2026.

5.9 5.9 Uncertainty and accelerating factors

Factor	Might **accelerate** CRQC	Might **delay** CRQC
Error-correction code advances	Breakthroughs in LDPC-surface hybrids	Diminishing returns in code discovery
Venture funding	Sustained VC + government subsidies	Investment winter post-2026
Geopolitical race	State-level moonshot funding (US, CN)	Export controls on cryogenics
Hardware yields	Photonic interconnect yields improve	Cryogenic supply-chain bottlenecks

Scenario planning (Appendix B) explores a "Fast-Track" case (CRQC = 2029) and "Delayed" case (CRQC = 2040) to stress-test organisational roadmaps.

5.10 5.10 Key takeaways for PAREK implementation

1. **Start now** – inventory and pilot migrations must commence by 2026 to remain compliant with EU roadmap.
2. **Assume shrinkage in threat horizon** – treat 2030 as plausible worst-case, not aspirational.
3. **Focus on data longevity** – prioritise assets whose confidentiality window extends into the 2030s.
4. **Engage suppliers early** – Section 13 outlines contract clauses; delays compound on CRQC acceleration.
5. **Invest in crypto-agility** – architectures that can hot-swap algorithms mitigate uncertainty.

5.11 5.11 References

1. Global Risk Institute (2024). *Quantum Threat Timeline Report 2024*.
2. Global Risk Institute (2025). *Quantum Threat Timeline 2025: Executive Perspectives*.
3. IBM (2024). *Roadmap to Quantum-Centric Supercomputers*.
4. IBM (2025). *The Era of Quantum Utility Is Here*.
5. NIST (2024). *Approval of FIPS 203, 204, 205*.

6. Keyfactor (2024). *Harvest Now, Decrypt Later*.
7. Marlink SOC Report (2025). *Harvest-Decrypt Incidents in Maritime Sector*.
8. Europol Quantum Safe Financial Forum (2025). *Recommendations to European Banks*.
9. SecurityWeek (2025). *Cyber Insights 2025 – Quantum and the Threat to Encryption*.
10. Gidney, C. & Ekerå, M. (2023). *How to Factor 2048-bit RSA Integers in 8 Hours with 20 Million Noisy Qubits*.

6 6 PQC Methodology

6.1 6.1 Purpose and position of this chapter

This methodology bridges the "**why**" articulated in the quantum-threat literature with the practical "**how**" codified in the PAREK framework. It supplies a repeatable lifecycle—*discover* → *assess* → *plan* → *execute* → *improve*—that any EU organisation can embed in its security management system and map onto the milestones of the Coordinated Implementation Roadmap (first-steps 2026, high-risk cut-over 2030, medium-risk completion 2035) .

6.2 6.2 Scientific foundation

Quantum risk geometry. Shor's and Grover's algorithms prove that once a *cryptographically-relevant quantum computer* (CRQC) exists, RSA/ECC and many symmetric-key constructions lose their assumed security margins. The most widely used quantitative model is the *Mosca Inequality*:

> **Tshelf-life + Tmigration > Tthreat your data will be exposed.**

The shelf-life of the data, the organisation's migration time, and the expert-assessed CRQC timeline must be evaluated together; breaches can begin long before a CRQC is built through *Harvest-Now-Decrypt-Later* (HNDL) attacks .

Expert forecasts. The 2024 Global Risk Institute survey of 32 quantum-hardware experts gives a median estimate of 11–15 years for a CRQC able to break RSA-2048, but with a heavy tail of earlier arrivals . Gidney & Ekerå's resource estimate (20 million noisy qubits, 8 hours) and subsequent error-

correction progress validate that such a machine is an engineering—rather than scientific—challenge . Because these forecasts shift annually, the methodology demands continuous refresh of *Tthreat*.

Standards landscape. In August 2024 NIST issued the first three Federal Information Processing Standards: FIPS 203 (ML-KEM / Kyber), FIPS 204 (ML-DSA / Dilithium) and FIPS 205 (SPHINCS+) . Forthcoming FIPS 206 (BIKE) and ISO/ETSI profiles will refine parameter sets, but the decision rule is already clear: design choices should default to these lattice- or hash-based schemes unless an explicit profile (IoT, constrained, statutory) dictates otherwise.

6.3 6.3 Design principles

1. **Crypto-agility first.** Because algorithm lifetimes are uncertain, architectures must allow hot-swapping of primitives without forklift upgrades .
2. **Inventory before surgery.** Every migration failure studied by TNO traced back to an incomplete asset list; hence inventory is a non-negotiable gate .
3. **Hybrid single-stack.** Where performance permits, run lattice-based KEMs or signatures *alongside* existing ECC/RSA until the latter can be fully retired. ETSI/IETF interop plug-tests show this halves rollback risk .
4. **Evidence over assertion.** Each stage outputs machine-readable artefacts—CBOMs, risk scores, migration run-books—that auditors and regulators can parse automatically.

6.4 6.4 Lifecycle phases

6.4.1 6.4.1 Phase 0 – Programme mobilisation

Although not counted among the five PAREK stages, a short mobilisation sprint (4–6 weeks) is advisable to assign roles, secure budget and ratify the scope statements defined in §3.

6.4.2 6.4.2 Phase 1 – Cryptographic discovery & inventory ("P" in PAREK)

Objective. Build a *single source of truth* describing every algorithm, key, certificate, protocol, hardware module and crypto-library instance.

Process.

- Crawl binaries and source trees with pattern-matching and dynamic-analysis tools.
- Enrich findings with network captures and certificate-transparency logs.
- Normalise results into a **Cryptography Bill of Materials (CBOM)**—an extension of CycloneDX 1.6—which supports >20 asset types (algorithm, protocol, key, seed, nonce, etc.) .
- Link CBOMs back to software SBOMs via *bom-link* URNs so each application instance can be traced to its crypto footprint .

Output artefacts.

- CBOM JSON (one per application or shared library)
- Discovery tooling report with false-positive triage
- Gap register listing unscanned networks or black-box third-party services

6.4.3 6.4.3 Phase 2 – Quantum risk assessment ("A")

Objective. Quantify urgency and migration difficulty, then classify systems into EU "high / medium / low" buckets.

Scoring model. Extend Mosca's inequality into a composite *Quantum-Adjusted Risk Score (QARS)*:

```
QARS = w1·(T_shelf-life / T_threat) + w2·(Migration_Cost / CapEx_Budget)
      + w3·(Data_Sensitivity) + w4·(Exposure_Surface)
```

where weights *w1–w4* are calibrated by sector regulators. TNO's handbook suggests default weightings of 0.35 / 0.25 / 0.25 / 0.15 after pilot workshops .

Scientific reference. Mosca & Mulholland's original risk methodology underpins the formula and justifies linear aggregation of shelf-life and migration vectors .

Output artefacts.

- Per-system risk dossier (QARS, assumptions, reviewer sign-off)

- Heat-map dashboard for C-suite and board reporting

6.4.4 6.4.4 Phase 3 – Road-mapping & readiness planning ("R")

Objective. Translate scores into dated, budgeted work-packages aligned with EU milestones.

Steps.

1. **Prioritise** systems with QARS 0.65 for immediate pilot migrations.
2. **Allocate buffer time** for external dependencies (e.g., hardware security modules awaiting FIPS 203 validation).
3. **Sequence pilots** to maximise knowledge reuse—start with a low-volume API gateway, then propagate the playbook to high-volume payment stacks.
4. **Integrate supplier clauses** requiring CBOM delivery and PQC-ready firmware by 2028 for high-risk contracts .

Output artefacts.

- Gantt chart or kanban milestones
- Budget breakdown: licences, hardware refresh, training, contingency
- Contract addenda language for suppliers

6.4.5 6.4.5 Phase 4 – Execution & migration ("E")

Objective. Replace—or wrap in hybrid mode—all quantum-vulnerable primitives, while preserving service levels.

Preferred migration patterns (scientific rationale in brackets):

- **Kyber-in-TLS 1.3 hybrid KEM:** Adds <2 kB to handshake; end-to-end field results show negligible latency increase at sub-10 ms RTT .
- **Dilithium signatures for code signing:** Larger certificates (~14 kB) but verified 100× faster than SPHINCS+, making it fit for CI/CD pipelines.
- **SPHINCS+ for long-life artefacts (firmware, legal archives):** Stateless hash-based design offers security with minimal cryptanalysis uncertainty.
- **Double-wrap archives:** Encrypt once with AES-256-GCM, then wrap the symmetric key via Kyber or BIKE to separate confidentiality from

PQC adoption pace.

Change-control safeguards. Each rollout includes a cryptographic *canary test*, real-time telemetry on handshake success rates, and a rollback plan tied to traffic shadowing.

Output artefacts.

- Migration run-books and playbooks per platform
- Performance-impact report versus baseline
- Certificate revocation & renewal schedule

6.4.6 6.4.6 Phase 5 – Key-governance & continuous improvement ("K")

Objective. Ensure that once migrated, systems stay quantum-resilient—even as algorithms evolve or new vulnerabilities surface.

Controls.

- **Continuous CBOM scanning:** Weekly delta scans detect drift; policy engines flag any newly imported RSA/ECC library versions .
- **Policy attestation via CycloneDX Attestations:** Suppliers attach machine-readable claims linking binaries to NIST/FIPS conformity, automating compliance checks .
- **Crypto-agility playbooks:** Design patterns (algorithm-independent keystores, versioned protocol negotiation, feature flags) enable hot re-parametrisation—a requirement emphasised by NCSC-NL and echoed in TNO Step 4.4 .
- **Metric suite:** Mean Time To Remediate Weak Crypto (MTTR-C), % assets with valid CBOM, % PQC certificates in production. These feed into ENISA reporting and, under NIS-2, into supervisory audits.

6.5 6.5 Embedding the methodology in EU governance

Member States' NIS Cooperation Group work-stream recommends each national roadmap publish quarterly status against the core measures above and contribute pilot results to the EU testing infrastructure . By harmonising metrics and artefacts (CBOM JSON, QARS spreadsheets, FIPS certificate IDs), the methodology enables cross-border comparability and pooled threat-intelligence.

6.6 6.6 Limitations and future research

While lattice-based KEMs currently lead standardisation, code-based (Classic McEliece) and isogeny-based (SIKE-like) schemes deserve niche consideration; the methodology therefore reserves an *Experimental Track* for low-volume prototypes. The scientific community is still refining fault-tolerance thresholds—e.g., the debate around "dynamic-logical qubits" may shift Tthreat earlier or later. Organisations must budget for annual model recalibration as these estimates mature.

6.7 6.7 Conclusion

This PQC Methodology equips EU organisations with a science-grounded, regulator-aligned and audit-ready pathway from cryptographic discovery to long-term quantum resilience. By anchoring every decision in measurable artefacts—CBOMs, risk scores, migration run-books—and iterating through the PAREK lifecycle, enterprises can defend today's and tomorrow's data against the quantum horizon.

7 7 Framework Overview

> **Purpose of this chapter** – give readers a *one-stop* visual and narrative tour of the PAREK Framework, explaining how its five stages interlock, what artefacts they exchange, and how the cycle repeats to deliver continuous crypto-agility.

7.1 7.1 At-a-glance diagram

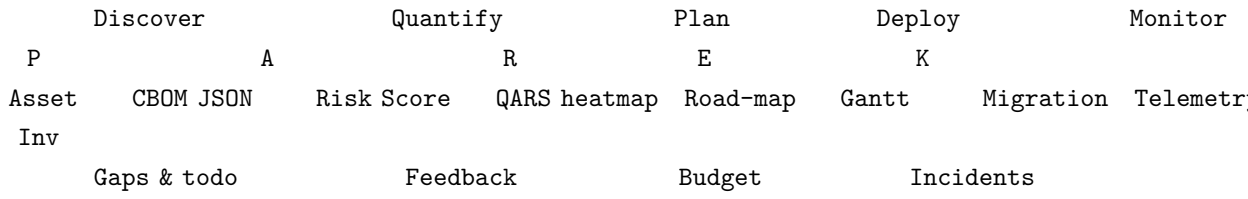


Figure 1 – PAREK Framework life-cycle (high-level data flow)

7.2 7.2 Stage synopses

7.2.1 7.2.1 P – Post-Quantum Asset & Algorithm Inventory

Goal – create a machine-readable **Cryptography Bill of Materials (CBOM)** for every software, hardware and service component. Uses automated scanners, manual surveys and supplier attestations. Output feeds directly into Stage A.

7.2.2 7.2.2 A – Assessment of Quantum Risk

Goal – compute a **Quantum-Adjusted Risk Score (QARS)** for each asset by blending data shelf-life, migration effort and CRQC timeline inputs. High-risk items graduate to Stage R while low-risk items loop back for periodic re-assessment.

7.2.3 7.2.3 R – Road-mapping & Readiness Planning

Goal – translate scores into a time-phased, resourced roadmap aligned to EU milestones (2026-2035). Outputs Gantt charts, budget forecasts, and supplier alignment plans. Detailed in §10.

7.2.4 7.2.4 E – Execution & Migration

Goal – deploy PQC or hybrid primitives using controlled roll-outs, rollback strategies and performance monitoring. Produces migration run-books and incident telemetry.

7.2.5 7.2.5 K – Key-Governance & Continuous Improvement

Goal – sustain crypto-agility through continuous scanning, supplier attestations, KPIs and policy refreshes. Feeds new discoveries back to Stage P, closing the loop.

7.3 7.3 Artefact hand-offs

From	To	Artefact	Format	Purpose
P	A	CBOMs (per system)	CycloneDX JSON + sig	Input for risk scoring

From To	Artefact	Format	Purpose
A R	QARS risk registry	CSV / Grafana feed	Prioritise backlog
R E	Work-package definitions	Jira Epics + Stories	Guide migration teams
E K	Deployment telemetry, incident reports	Prometheus / GRC logs	Measure success, trigger alerts
K P	Revised asset list, KPIs	JSON diff, dashboard	Refresh inventory & repeat cycle

7.4 7.4 Governance layers

7.4.1 7.4.1 Strategic layer

PAREK Steering Committee (quarterly) endorses roadmaps, budget, and policy changes.

7.4.2 7.4.2 Operational layer

Crypto Working Group (monthly) coordinates cross-team dependencies, tooling upgrades and incident response.

7.4.3 7.4.3 Tactical layer

Dedicated *Migration Squads* execute Jira stories, report blockers and feed metrics to dashboards.

7.5 7.5 Alignment with PQC Methodology (§6)

Section 6 introduces the **discover → assess → plan → execute → improve** cycle at conceptual level. This chapter grounds that abstract model in concrete artefacts, roles and data flows, forming the *Rosetta Stone* that maps theory to practice.

Key alignment points:

- **Inventory before surgery** principle manifests as the strict P A gate.
- **Crypto-agility first** translates into K metrics (# low-risk ECDSA certs trending → 0).

7.6 7.6 Integration with supply-chain (§13)

Supplier CBOMs are imported into Stage P; supplier roadmaps and compliance clauses sit in Stage R; supplier attestation SLAs are monitored in Stage K. Thus, the framework treats third-party components as *co-equal citizens* in the life-cycle.

7.7 7.7 Quality gates & escalation paths

```
[Gate G1] CBOM coverage  95 % - proceed to Stage A  | else: raise Inventory CAPA
[Gate G2] QARS sign-off by CISO - proceed to Stage R  | else: re-score anomalies
[Gate G3] Budget approval - proceed to Stage E      | else: escalate to CFO
[Gate G4] KPI trend green 3 months - close loop     | else: open incident review
```

Each gate has an *owner*, *entry criteria* and *exit criteria*, ensuring accountability.

7.8 7.8 Toolchain reference stack

Stage	Open-source baseline tools	Commercial alternatives
P	**oqs-scanner**, `cyclonedx-python-lib`	Venafi TLS Protect, Fortanix DSM
A	`pandas + risk-calc.py`	RSA Archer, ServiceNow VRM
R	`ganttlab`, GitLab Road-maps	Atlassian Advanced Roadmaps
E	`openssl-oqs`, QEMU testbed	Entrust nShield, Thales CipherTrust
K	Grafana, Prometheus	Splunk ES, Elastic SIEM

A Terraform module (`scripts/terraform/parek-stack.tf`) provisions the open-source stack for pilots.

7.9 7.9 Maturity model

Level	Characteristics	Typical KPI values
1 – Ad hoc	No CBOM, PQC unknown, vendors unmanaged	SC-1 $<10\,\%$
2 – Defined	Static inventory, pilot QARS, roadmap draft	SC-1 50 %, QARS cov. 30 %

Level	Characteristics	Typical KPI values
3 – Managed	Approved roadmap, hybrid pilots in prod	SC-1 90 %, KPI trend ↑
4 – Quantitative	Real-time metrics, full PQC for high-risk assets	KPI SLA 5 % viol.
5 – Optimising	Continuous crypto-agility, auto-rotation	Zero unsupported algs

Stage K owns the maturity assessment and reports progression each quarter.

7.10 7.10 Next steps for readers

- **Architects** – dive into §8–12 for deep-dive guidance per stage.
- **Project managers** – reference §10 for detailed timelines and resource models.
- **Suppliers** – jump to §13 for contract clauses and CBOM spec requirements.

8 8 P – Post-Quantum Asset & Algorithm Inventory

Purpose – provide a succinct overview of how to catalogue all cryptographic assets and algorithms so that subsequent risk scoring (Stage A) is based on complete, reliable data. This short version is intended as a quick-start guide; a full procedural manual will follow in v0.2.

8.1 8.1 What is a CBOM?

A **Cryptography Bill of Materials (CBOM)** is a machine-readable inventory (CycloneDX JSON) listing every algorithm, key, certificate, protocol and crypto-module used by a software, hardware or service component. Think of it as an SBOM for cryptography.

8.2 8.2 Minimal discovery workflow

Step	Action	Tool / Source	Output
1	Binary & source code scan	`oqs-scanner`, regex	Algorithm list
2	Network traffic sampling	Zeek, Wireshark	Cipher-suite map
3	Certificate inventory	CT logs, PKI DB	x509 dump
4	Supplier CBOM ingest	API / S3 / email (§13)	External JSON
5	Manual survey for edge assets	Google Forms	Gap register

Run steps 1–4 in parallel; perform step 5 only if coverage $< 95\,\%$.

8.3 8.3 Essential data fields

1. `algorithm` – e.g., `rsa2048`, `ml-kem-768`
2. `context` – `tls1.3`, `ssh2`, `jwt`
3. `keySize` / `parameterSet`
4. `usage` – signing, encryption, key agreement
5. `expires` – ISO date for certificates/keys
6. `hardwareAnchor` – HSM/TPM model + firmware

Include a `scanTimestamp` and digital signature (`*.cbom.sig`).

8.4 8.4 Quality gate G1 (inventory lock)

- **Metric** – % assets with valid CBOM 95 %.
- **Owner** – Asset-Inventory Lead.
- **Tool** – Grafana dashboard `CBOM-coverage`.

If coverage $< 95\,\%$, raise Corrective Action Plan and block Stage A.

8.5 8.5 Outputs

- **CBOM repository** – `git@repo:cbom/` with one JSON per system.
- **Gap register** – CSV of unscanned or unknown assets.
- **Coverage dashboard** – auto-refreshed via Prometheus.

8.6 8.6 Common pitfalls

1. **Duplicate asset IDs** – enforce UUID naming.
2. **Missing hardware mapping** – integrate CMDB export.
3. **Supplier lag** – tie CBOM submission to invoice milestone.

8.7 8.7 Next steps

Once G1 is passed, hand off the consolidated CBOM set to Stage A for QARS calculation. Retain automated nightly scans to catch drift.

9 9 A – Assessment of Quantum Risk

> **Purpose of this chapter** – define a repeatable, data-driven methodology for quantifying how urgently each system, data set or supplier must migrate to post-quantum cryptography. The output of this stage—**Quantum-Adjusted Risk Scores (QARS)**—feeds Road-mapping (§10) and underpins budget and resource prioritisation.

9.1 9.1 Why risk scoring matters

Cryptographic migration budgets are finite, systems are heterogeneous, and CRQC timelines are uncertain. A robust risk model ensures that *business-critical, long-lived* data is protected first, while low-impact assets follow a just-in-time trajectory. Without quantification, organisations either under-invest (and face data-exposure liability) or over-invest (and stall other security priorities). The QARS model harmonises quantitative (years, euros, CVSS-scores) and qualitative (business impact, regulatory penalty) inputs into a single comparable metric.

9.2 9.2 Inputs and prerequisites

Input	Source	Refresh cadence
Cryptography Bill of Materials (CBOM)	Stage P (§8)	Nightly
Data-classification registry	GDPR/NIS-2 policy owners	Quarterly
CRQC threat horizon (`T_threat`)	§5 + external forecasts	Annual + ad hoc
Migration effort estimates	Architecture & dev-ops	Sprintly
Exposure Surface Index (ESI)	Pentest/vuln-scan teams	Monthly

If any CBOM asset lacks a data-classification tag or migration estimate, it is flagged "information incomplete" and cannot be scored until gaps are resolved.

9.3 9.3 The QARS formula

PAREK extends Mosca's inequality into a **multi-factor linear model**:

```
QARS = w ·(T_shelf / T_threat) + w ·(T_migration / T_buffer) + w ·Data_Sensitivity +
       w ·Exposure_Surface + w ·Compliance_Penalty
```

Symbol	Explanation	Scale
`T_shelf`	Required confidentiality window (years)	0–25+
`T_threat`	Forecast years until CRQC (default = 9–15)	0–20
`T_migration`	Estimated time to complete PQC rollout (yrs)	0–5
`T_buffer`	Policy-set buffer (yrs, default = 2)	fixed
`Data_Sensitivity`	GDPR Level 1-3 or internal A-E scale	0.1-1
`Exposure_Surface`	Normalised count of public endpoints & CVEs	0-1
`Compliance_Penalty`	0.2 if asset falls under NIS-2 critical infra	0/0.2

Weights `w …w` default to **0.30 / 0.20 / 0.25 / 0.15 / 0.10** but can be re-tuned at sector level (e.g., finance may increase sensitivity weight to 0.35). QARS outputs a **unitless value between 0 and 1** where $0.65 =$ *high*, 0.35–0.64 = *medium*, $< 0.35 =$ *low*.

9.4 9.4 Data-collection pipeline

1. **Ingest** – nightly ETL job pulls CBOM JSON, joins CMDB IDs, merges data-classification tags.
2. **Enrich** – scrape CVE feeds (NVD) to calculate Exposure Surface Index for IP addresses/certs.
3. **Estimate** – dev-ops provides story-point-based migration effort which converts to months via team velocity.
4. **Compute** – Python microservice (`scripts/qars_calc.py`) applies formula; outputs per-asset records to Postgres and Grafana.
5. **Validate** – security architects review anomalies (e.g., QARS > 0.9 for "low" data system) via Jira workflow.

All stages run in a dedicated Kubernetes namespace with signed container images; audit logs export to Splunk for regulator access.

9.5 9.5 Visualising risk

Default dashboards include:

- **Heat-map** – assets on x-axis (systems) vs. y-axis (QARS); colour gradient highlights urgency.
- **Scatter** – `T_shelf` on x, `T_migration` on y; diagonal line shows Mosca boundary.
- **Burndown** – number of high-risk assets over time; target trend = zero by Q4 2030.

Grafana JSON for these panels is stored under `assets/grafana/qars_dash.json`.

9.6 9.6 Quality gate G2 – QARS sign-off

Before Stage R can commence, the CISO (or delegate) must approve:

1. **Coverage** – $\geq 90\,\%$ of in-scope assets have non-null QARS.
2. **Accuracy** – sample audit ($10\,\%$) shows $< 5\,\%$ variance between estimated and observed parameters.
3. **Documentation** – methodology, weight settings, data sources captured in Confluence page `PQC/Risk-Method`.

Failure to meet criteria pauses migration planning; corrective actions logged in the *Risk Management* Jira project.

9.7 9.7 Scenario analysis

PAREK requires bi-annual **scenario runs** to test sensitivity:

Scenario ID	`T_threat` assumption	Outcome metric	Implication
S-A (Fast)	5 yrs (2029)	ΔHigh-risk assets + 35 %	Budget re-prioritisation needed
S-B (Baseline)	Median 9 yrs (2034)	n/a	Reference roadmap
S-C (Delayed)	15 yrs (2040)	ΔBudget – 18 %	Optional slow-track for low assets

Results feed the CFO's risk-adjusted cost model; Stage 10 picks whichever roadmap keeps high-risk completion <= 3 yrs before `T_threat`.

9.8 9.8 Integration with supplier risk

Supplier CBOMs (Tier 1 & 2) receive QARS as well. Additional factor `Supplier_Maturity` (scale 0–0.2) reduces QARS if vendor demonstrates crypto-agility lab results. Non-compliant suppliers auto-escalate to *Supplier Risk Queue* (§13) and may face contract penalties.

9.9 9.9 Common pitfalls & mitigations (100 words)

1. **Stale data** – automate nightly refresh; raise alert if CBOM timestamp > 7 days.
2. **Weight gaming** – lock weights quarter-by-quarter; require Steering approval for changes.
3. **False precision** – present score bands (high/med/low) to execs, not raw decimals.
4. **Blind spots** – add "Unknown" category and track reduction KPI.

9.10 9.10 Outputs

- `risk_registry.csv` – asset-level QARS, drivers, timestamp.
- Grafana dashboard – URL `/d/qars/quantum-risk`.
- Executive slide deck template (`assets/templates/qars-brief.pptx`).

9.11 9.11 Next steps

Hand off risk-registry to Stage R for roadmap planning. Schedule next scenario analysis within 6 months or sooner if IBM announces 1 M qubits.

9.12 9.12 References

1. Mosca, M. (2023). *Risk Framework for Quantum Threats*.
2. Global Risk Institute (2024). *Quantum Threat Timeline Report*.
3. ENISA (2024). *Good Practices for Supply-chain Risk Management*.
4. NIST (2024). *Post-Quantum Cryptography FIPS 203-205*.
5. IBM (2025). *Quantum Roadmap*.

10 10 R – Road-mapping & Readiness Planning

> **Purpose of this chapter** – translate the quantitative urgency produced in *§9 Assessment of Quantum Risk* into a resourced, dated and regulator-aligned action plan that will deliver quantum resilience across the organisation's entire technology estate.

10.1 10.1 Scope and positioning

Road-mapping and readiness planning (the **R** in *P-A-R-E-K*) is the linchpin phase that turns analytical findings into concrete, executive-approved commitments. It spans three macro tasks:

1. **Prioritise** – decide which systems, business services and supply-chain partners move first, based on QARS scores, EU risk categories and practical constraints;
2. **Plan** – build a realistic programme schedule with phased deployments, governance checkpoints and budget allocations; and
3. **Prepare** – ensure that people, processes and technology are in place when execution starts (tooling, contracts, training, fallback strategies).

The output is a *single authoritative roadmap* that boards, regulators and suppliers can cite. Without it, migration efforts splinter into ad hoc projects that stall or overrun.

10.2 10.2 Key inputs

Artefact	Source section	Description
CBOM inventory	§8	Machine-readable list of algorithms, keys and protocols per system
QARS scores	§9	Composite urgency rating (0–1) per system/service
EU roadmap milestones	External	2026 early pilots, 2030 high-risk cut-over, 2035 medium-risk completion
Budget envelope	CFO	Multi-year capital & operational funding ceiling
Resource capacity	HR / PMO	Available FTEs, external consultants, supplier bandwidth

10.3 10.3 Process overview

```
          1                    2                3
Risk & Asset       Prioritisation       Road-map Plan       Readiness Set
 Intelligence
(§8 & §9)           (10.4)                (10.5)             (10.6)
```

Each arrow represents a *quality gate* – the roadmap cannot progress until the preceding artefacts are baseline-approved.

10.4 10.4 Step 1 Prioritisation (4 weeks)

The goal is an **ordered backlog** of migration work-packages.

10.4.1 10.4.1 Segmentation

- **Risk bucket** – map QARS 0.65 to *high*, 0.35–0.64 to *medium*, < 0.35 to *low*.
- **Business criticality** – overlay impact tiers (mission-critical, regulatory, customer-facing, internal).

- **Dependency heat-map** – identify technical couplings (shared crypto libraries, common PKI roots, hardware modules).

10.4.2 10.4.2 Scoring matrix

Create a *Prioritisation Index (PI)* = `w_risk × QARS + w_imp × Impact + w_dep × Coupling`. Default weights 0.4 / 0.4 / 0.2 can be tuned in steering committee.

10.4.3 10.4.3 Pilot selection

Select at least one representative workload in each domain (web, mobile, embedded, data-at-rest) to validate migration playbooks. Early pilots should have: * 10 k TPS (to limit blast radius) * Dedicated dev-ops pipeline for rapid iteration * Supportive product owner

10.5 10.5 Step 2 Road-map planning (6 weeks)

This step converts the ordered backlog into a **multi-year, resource-levelled Gantt**.

10.5.1 10.5.1 Timeline alignment

Milestone	EU target	Local target	Notes
Inventory baseline	2026-03-31	2026-03-15	lock CBOM scope
Pilot migrations live	2026-12-31	2026-11-30	include telemetry & rollback
High-risk systems PQC-ready	2030-12-31	2030-06-30	6-month buffer for audit
Medium-risk systems PQC-ready	2035-12-31	2035-06-30	contingent buffer

Rationale – buffer dates absorb supplier slippage, new standard releases (FIPS 206, ISO/ETSI), or geopolitical disruptions.

10.5.2 10.5.2 Work-package design

Break down migrations into **Epics** (e.g., *TLS Stack Upgrade*) and **Stories** (e.g., *enable hybrid Kyber in nginx 1.25*). Attach: * Definition of Done (test cases, security sign-off) * Estimated story points & duration * Owner team and SME reviewers

10.5.3 10.5.3 Capacity & cost modelling

- **FTE mapping** – match story points to sprint velocity.
- **External spend** – licences, new HSMs, PKI vouchers, test-bed cloud costs.
- **Contingency reserve** – 15 % of total CapEx based on Monte Carlo simulation of schedule risk.

10.5.4 10.5.4 Governance calendar

Publish quarterly steering reviews and monthly working-group checkpoints. Each high-risk migration has a *go/no-go gate* with rollback cut-off defined.

10.6 10.6 Step 3 Readiness preparation (ongoing)

10.6.1 10.6.1 Supplier alignment

- Embed *PQC-ready clause* requiring CBOM + SPDX attestation with FIPS-cert IDs by 2028.
- Incentivise via payment milestones – 10 % retainage until PQC compliance confirmed.

10.6.2 10.6.2 Toolchain hardening

Tool category	Minimum capability
CI/CD scanner	Detect lattice or hash-based algorithm support, block RSA-2048 certs
Traffic analyser	Real-time handshake cipher suite telemetry
HSM firmware	Supports ML-KEM-768, ML-DSA-5, hybrid wrapping

10.6.3 10.6.3 Skills uplift

Deliver a role-based training matrix: * **Dev-ops** – PQC libraries, hybrid handshake patterns (2-day workshop) * **IT Ops** – firmware-signing, key rotation (1-day lab) * **Risk officers** – QARS methodology, reporting dashboard (webinar + playbook)

10.6.4 10.6.4 Fallback planning

Run *table-top exercises* for: 1. PQC handshake failure in production causing 5xx spike. 2. Upstream library CVE requiring emergency algorithm swap. 3. Supplier unable to deliver CBOM by contractual date.

Each scenario results in a *response run-book* with RACI mapping and MTTR target.

10.7 10.7 Outputs and deliverables

- **Master roadmap** (interactive Gantt or Kanban) stored in PMO repository.
- **Budget & resource plan** linked to finance system cost centres.
- **Supplier tracker** – contract ID, CBOM status, PQC clause compliance.
- **Risk-adjusted timeline** – spreadsheet showing QARS, PI, and planned migration date per asset.

All deliverables should version via Git (for content) and SharePoint/Confluence (for presentation decks). Use semantic version tags (e.g., `roadmap-v1.1.0`) to sync with Document Control.

10.8 10.8 Quality gates & KPIs

Gate	Artefacts required	Approver	KPI trigger
G1 – Inventory lock	CBOM freeze, gap register	CISO	$< 95\,\%$ asset coverage
G2 – Pilot go-live	Run-book, rollback plan, test report	Head of Ops	Error rate $> 0.1\,\%$

Gate	Artefacts required	Approver	KPI trigger
G3 – High-risk cut-over	External audit attestation	Regulator liaison	Audit finding severity > "medium"
G4 – Programme closure	Lessons-learned report, metrics dashboard	Board	MTTR-C > 30 days

Key performance indicators track *Predictability* (variance vs. baseline), *Quality* (defects, CVEs), and *Crypto-compliance* (% PQC certs).

10.9 10.9 Common pitfalls & how to avoid them

1. **Over-reliance on vendor roadmaps** – mitigate by testing open-source PQC libraries in parallel.
2. **Ignoring hidden dependencies** (e.g., SSO tokens signed with RSA) – mandate *dependency graph export* before migration.
3. **Resource starvation** during long tail of low-risk systems – secure multi-year budget with ring-fenced FTEs.
4. **One-shot big-bang** migrations – favour *incremental hybrid* roll-outs with fast rollback.
5. **Communication gaps** – publish monthly progress dashboards to executives and teams.

10.10 10.10 References

- European Union (2025). *Coordinated Implementation Roadmap for Post-Quantum Cryptography.*
- TNO (2024). *Post-Quantum Cryptography Handbook.*
- NIST (2024). *FIPS 203, 204, 205.*
- Mosca, M., et al. (2023). "Cloud migration timelines for quantum risk".

11 11 E – Execution & Migration

Purpose of this chapter – provide a practical playbook for migrating systems from quantum-vulnerable cryptography to post-quantum or hybrid primitives while maintaining service continuity, performance, and compliance. It covers deployment models, testing strategies, rollback procedures and quality gates.

11.1 11.1 Guiding principles (120 words)

1. **Hybrid first** – pair PQC primitives with existing RSA/ECDHE until ecosystem maturity allows full cut-over.
2. **Incremental roll-out** – deploy to a small blast radius, monitor, then expand.
3. **Telemetry-driven** – measure handshake success, latency, error rates in real time.
4. **Reversible** – every deployment must include an automated rollback path.
5. **Compliance aligned** – FIPS-approved parameter sets, algorithm policy enforced via crypto providers.

11.2 11.2 Migration patterns (250 words)

Pattern ID	Use case	Description	Pros	Cons
M-H-TLS	Web/API TLS traffic	TLS 1.3 hybrid KEM: X25519 + ML-KEM-768 (RFC 9399)	Minimal latency; browsers in test builds	Larger ClientHello (~3 kB)
M-H-SSH	Admin shell access	OpenSSH 9.4c with ECDH-SHA2 + Kyber768 + dilithium keys	Easy CI integration	Requires updated clients
M-PKI-Nested	Code signing	RSA-2048 + Dilithium cert chain (nested signatures)	Backwards compatible	2× cert size

Pattern ID	Use case	Description	Pros	Cons
M-Hash-IoT-FW	Long-life firmware updates	SPHINCS+ (128s) detached signature; verify in bootloader	Stateless, audit-friendly	1 MB signature size
M-Sym-Wrap	Large data archives	AES-256-GCM data, key wrapped with Kyber1024 then stored	Separates data-at-rest from PQC cadence	Key management overhead

11.3 11.3 Deployment workflow (200 words)

1. **Readiness checkpoint** – ensure Stage R work-package passes go/no-go gate.
2. **Pre-prod lab** – replicate production traffic with synthetic load; collect baseline metrics.
3. **Canary release** – enable PQC for 1 % of traffic or a single AZ/node.
4. **Observation window** – monitor KPIs (handshake success 99.9 %, latency +5 ms).
5. **Gradual ramp-up** – double traffic every 24 h if KPIs green.
6. **Full rollout** – 100 % production traffic.
7. **Post-deployment audit** – verify cert chains, scan for deprecated algorithms.

Automated scripts (`scripts/deploy/hybrid_tls.sh`) orchestrate feature flags via Envoy or nginx annotations.

11.4 11.4 Testing strategy (180 words)

Test type	Tool / framework	Success criterion
Unit tests	Google Test / Catch2	PQC library returns expected ciphertext length
Integration tests	Docker Compose stack	Service handshake completes in < 100 ms

Test type	Tool / framework	Success criterion
Fuzz testing	libFuzzer + AFL++	No crashes after 24 h fuzzing
Interop tests	OQS-OpenSSL OQS-nginx	100 % pass across selected cipher suites
Performance bench	wrk2, k6, vegeta	Throughput impact 5 % of baseline
Chaos drills	Pumba / TC-netem	Rollback trigger within 30 s of error spike

Continuous Integration pipelines in GitLab run these stages; results export to SonarQube and Grafana.

11.5 11.5 Rollback & contingency (120 words)

Every deployment artefact includes: - **Feature flag** to disable PQC handshake at runtime. - **Blue/green** or **canary** deployment environment. - **Backup certificates/keys** staged and tested. - **Automated playbook** `scripts/rollback/hybrid_tls_revert.sh`.

Triggers: - Error rate $> 0.5\,\%$ sustained for 5 min. - Latency increase > 50 ms for 5 min. - Security incident flagged by SOC.

11.6 11.6 Telemetry & metrics (150 words)

Metric ID	Description	Target	Collector
E-1	PQC handshake success rate	99.9 %	Envoy stats
E-2	Median handshake latency (ms)	+5 ms	Prometheus
E-3	Error 5xx ratio during rollout	0.1 %	Loki logs
E-4	Deprecated cipher usage (per hour)	0	Zeek

Dashboards live at `Grafana > PAREK > Execution`.

11.7 11.7 Quality gate G3 – Production readiness (80 words)

CISO (security), CIO (availability) and CFO (budget) sign off when: 1. All tests pass, KPIs within thresholds. 2. Backout plan validated in staging. 3. Supplier HSM firmware certs present. 4. Compliance evidence (FIPS cert numbers) attached to release ticket.

11.8 11.8 Documentation deliverables (100 words)

- **Migration run-book** – step-by-step with screenshots/log snippets.
- **Risk acceptance record** – signed PDF by risk owner.
- **Change record** – ITIL ticket with links to pipeline run IDs.
- **Post-implementation review** – lessons learned, metric screenshots.

Stored in `Confluence > PQC > Execution` with version tags matching Git tags.

11.9 11.9 Common pitfalls & mitigations (120 words)

1. **TLS library mismatch** – pin exact OQS-OpenSSL version; run interop tests.
2. **Certificate-size blow-up** – enable TLS 1.3 compression extensions or nested certs.
3. **Log parser breakage** – update regex patterns to parse new cipher suite names.
4. **HSM queue overflow** – capacity test firmware before prod.
5. **Shadow RSA glue code** – static-link scanners in CI.

11.10 11.10 Future roadmap (90 words)

- **Full PQ-only mode** once browser vendors ship Kyber in stable channels (target 2029).
- **Algorithm agility APIs** (e.g., libpqcrypto v2) to hot-swap parameter sets.
- **Quantum-safe VPN and email encryption pilots** (Stage E-2026-Q4).

11.11 11.11 References

1. IETF (2023). *RFC 9399 – Hybrid Key Exchange in TLS 1.3*.
2. Open Quantum Safe (2024). *OQS-OpenSSL 4.1*.

3. NIST (2024). *FIPS 203 / 204 / 205*.
4. ENISA (2025). *Post-Quantum Migration Patterns*.

12 12 K – Key-Governance & Continuous Improvement

Purpose of this chapter – define how EU-based organisations maintain crypto-agility, monitor post-quantum cryptography (PQC) compliance, and sustain supplier accountability after initial migrations are complete. Governance mechanisms align with **NIS 2**, **DORA**, **GDPR**, the forthcoming **EU Cyber Resilience Act (CRA)**, and ENISA good-practice guidelines.

12.1 12.1 Governance objectives (100 words)

1. **Assurance** – demonstrate to EU supervisory authorities (e.g., NIS Cooperation Group, ECB-SSM, EBA) that PQC controls remain effective.
2. **Transparency** – provide board-level and regulator-level dashboards for cryptographic health.
3. **Continuous agility** – support hot-swaps to new PQC algorithms (e.g., ML-KEM→ML-KEM-1024) without business disruption.
4. **Incident resilience** – detect, triage and remediate crypto failures within predefined Mean Time to Remediate Crypto (MTTR-C) targets.

12.2 12.2 Organisational structure (150 words)

Body	Frequency	Mandate	EU reference
PAREK Steering Committee	Quarterly	Approve metrics, budget, policy updates	NIS 2 Art.20 (management oversight)

Body	Frequency	Mandate	EU reference
Crypto Governance Office (CGO)	Monthly	Operate dashboards, coordinate audits, own algorithm policy	ENISA Good Practice 4.2
Crypto Review Board (CRB)	Ad hoc	Assess new algorithms/parameters, sanction emergency swaps	ETSI TS 119 996 input
Supplier Cryptography Board (SCB)	Quarterly	Review Tier-1 supplier attestation and CBOM status	CRA Art.35 (supplier obligations)

Role mappings live in `part3/14-raci.md`.

12.3 12.3 Policy stack (120 words)

1. **Cryptographic Policy (CP-01)** – lists approved algorithms, key lengths and protocols; revision every 6 months.
2. **Key Management Standard (KMS-EU-02)** – describes lifecycle (generation, storage in EU Qualified Trust Service Provider (QTSP) HSMs, rotation, destruction).
3. **Algorithm Deprecation Procedure (ADP-03)** – triggers, timelines and communication templates for banning weak algorithms.
4. **Supplier Cryptography Policy (SCP-04)** – references §13 PQC Annex, aligns with CRA Article 10.

Policies are version-controlled in Git (`/policy/*`) and published to the intranet Confluence space `PQC/Policies`.

12.4 12.4 Metrics & KPIs (200 words)

KPI ID	Metric	Target	EU linkage
K-1	% Assets with valid CBOM (< 24 h old)	98 %	CRA Art.23 (SBOM/CBOM)
K-2	Unsupported algorithm instances detected	0	NIS 2 Art.21 (technical measures)
K-3	Mean Time to Remediate Crypto (MTTR-C)	30 days high-risk; 90 days medium	DORA RTS on ICT risk
K-4	% Supplier attestations received on time	95 %	CRA Art.35
K-5	Annual crypto penetration test coverage	100 % Tier-1, 80 % Tier-2	EBA Guidelines (ICT security)

All KPIs surface in Grafana dashboard `PQC > Governance > EU Metrics` and feed quarterly NIS 2 reports.

12.5 12.5 Continuous CBOM scanning (150 words)

A **CBOM Delta Scanner** (Rust microservice) polls the CBOM graph database hourly, compares it with the last approved baseline and flags: - **Additions** – new algorithms or keys not in policy. - **Deletions** – removed assets (possible shadow IT). - **Parameter drift** – changed key size or version.

Alerts integrate with ServiceNow (CIRF module). False positives must be closed within 72 h. All deltas export to `assets/reports/cbom-delta-YYYY-MM-DD.csv` for audit evidence.

12.6 12.6 Algorithm lifecycle management (180 words)

12.6.1 12.6.1 Evaluation pipeline

1. **Research Intake** – CGO tracks NIST, ETSI, CEN/CENELEC outputs.
2. **Lab benchmark** – CRB benchmarks latency, CPU, memory on reference workloads.
3. **Security review** – external academic peer review (EU PQC Consortium).
4. **Pilot flag** – enable new algorithm behind feature flag for selected services.
5. **Policy update** – if successful, CP-01 revision published.

12.6.2 12.6.2 Deprecation stages

Stage	Marker	Timeline
Proposed	New candidate algorithm in ETSI draft	0 months
Approved	Added to CP-01	+6 mths
Mandatory	Required for all new deployments	+18 mths
Forbidden	Outgoing algorithm banned	+36 mths

Communication packs sent via email and intranet; affected product owners get Jira tasks auto-generated.

12.7 12.7 Incident response & reporting (150 words)

Crypto incidents are handled under the **EU NIS 2 major incident** framework:

1. **Detection** – SOC rule "unsupported_ciphersuite" fires.
2. **Initial report** – Incident Response Team logs case in TheHive; notif to national CSIRT within 24 h.
3. **Containment** – activate rollback script or key rotation.
4. **Eradication** – remove bad certs, patch firmware.
5. **Post-incident report** – deliver ENISA-template report within 72 h to competent authority.
6. **Lessons-learned review** – CRB updates ADP-03 or KMS-EU-02.

All steps timestamped; evidence archived in EU datacentre (GDPR compliant).

12.8 12.8 Audit & assurance (120 words)

- **Internal audit** – annual review aligned with ISAE 3402, reports to Audit Committee.
- **External audit** – Big 4 or qualified auditor validates KPIs, CBOM process, compliance with CRA and NIS 2.
- **Regulator review** – ECB-SSM may request additional evidence for systemically important banks; DORA mandates ICT third-party risk audits.

Audit findings tracked in Jira project `AUDIT-PQC`; remediation owned by CGO.

12.9 12.9 Integration with other PAREK stages (100 words)

- **From Stage E** – deployment telemetry populates KPIs K-1 to K-3.
- **To Stage P** – CBOM deltas feed new asset discovery.
- **To Stage R** – maturity scores influence roadmap reprioritisation.
- **With Stage A** – incident metrics adjust Exposure Surface Index for QARS re-runs.

12.10 12.10 Future EU developments (80 words)

The **EU Digital Identity Wallet** regulation (eIDAS 2) will require PQC-capable Qualified Electronic Signatures (QES) by 2030. The **EU AI Act** may impose additional controls for cryptographic integrity in AI systems. Governance policy CP-01 plans review cycles aligned to these legislative sunsets.

12.11 12.11 References

1. ENISA (2025). *Good Practices for Crypto-Agility and Post-Quantum Preparedness.*
2. European Commission (2023). *NIS 2 Directive.*
3. European Parliament (2025). *Cyber Resilience Act – final text.*
4. ECB-SSM (2024). *Cyber Resilience Oversight Expectations for FMIs.*
5. ETSI (2024). *TS 119 996 – Algorithm Agility Guidance.*
6. CEN/CENELEC (2025). *PQC Standards Roadmap.*

13 13 Supply-Chain Integration

Purpose of this chapter – embed post-quantum cryptography (PQC) requirements into the entire supplier life-cycle so that every external component, cloud service and piece of hardware entering the organisation's environment supports PAREK objectives and timelines.

13.1 13.1 Why supply-chain matters in the quantum era

Modern digital estates are a mosaic of proprietary SaaS APIs, open-source libraries, OEM devices and managed service providers. Research by ENISA shows that 75 % of successful crypto-deprecation projects failed **not** because internal teams resisted change but because third-party dependencies lagged two to three years behind security roadmaps. Quantum migration exacerbates this risk: a single RSA-signed software update from a vendor can re-introduce vulnerable primitives across thousands of endpoints. Therefore, PQC adoption is no longer an internal programme but a **supply-chain transformation endeavour**. Section 13 defines the contractual hooks, technical artefacts (CBOM/SBOM), validation workflows and governance forums required to make suppliers first-class citizens in the PAREK lifecycle.

13.2 13.2 Scope and definitions

Supplier means any external legal entity that designs, builds, sells or operates software, hardware or services running in, or interfacing with, the organisation's production or pre-production environments. This includes SaaS providers, IaaS/PaaS cloud vendors, OEM hardware suppliers, open-source project maintainers (where code is bundled), consultants and contract developers. **Supply-chain integration** spans four control layers: *onboarding*, *contracting*, *operation*, and *termination*. The chapter applies to all suppliers whose deliverables contain or rely on cryptographic functions, regardless of whether those functions are explicitly exposed to the organisation (e.g., TLS) or hidden inside firmware.

13.3 13.3 Objectives

1. **Cryptographic transparency** – every supplier must furnish a machine-readable Cryptography Bill of Materials (CBOM) aligned to

CycloneDX v1.6.

2. **PQC readiness** – high-risk suppliers deliver PQC-capable builds by 2028; medium-risk by 2031.
3. **Continuous assurance** – suppliers attest quarterly that no unsupported algorithms (RSA 2048, ECC P-256, SHA-1) appear in deliverables.
4. **Incident response** – suppliers notify the organisation within 24 hours of any crypto-related CVE with a CVSS score 7.0.

13.4 13.4 Supplier segmentation model

The organisation classifies suppliers into **three tiers**:

Tier	Criteria	Examples	Governance cadence
1 – Strategic	Provides mission-critical platforms or handles classified data.	Core banking engine, national ID cloud.	Quarterly steering; on-site audits.
2 – Operational	Supports key business processes but without systemic impact.	CRM SaaS, managed network.	Semi-annual review; remote audit.
3 – Commodity	Easily replaceable, low data sensitivity.	Peripheral hardware, bulk email gateway.	Annual self-assessment.

The tier determines the depth of CBOM detail, test evidence, and contract clauses required. Tier 1 suppliers must present signed CBOMs, PQC migration roadmaps and evidence of internal crypto-agility testing. Tier 3 suppliers may supply a simplified attestation if they leverage a certified Tier 1 sub-provider.

13.5 13.5 Contractual requirements

All new or renewed contracts **must** include a *PQC Annex* covering:

1. **CBOM delivery schedule** – initial CBOM within 30 days of contract signature; refreshed artefact with each major release or monthly for SaaS.
2. **PQC migration milestones** – align with the organisation's roadmap (§10):
   - Kyber/Dilithium hybrid capability in test by **2027-12-31**.

- FIPS-validated PQC primitives in production by **2030-06-30** for Tier 1; **2031-12-31** for Tier 2.

3. **Algorithm deprecation clause** – supplier shall not introduce or re-enable algorithms listed on the organisation's *Forbidden Algorithm List* (FAL).
4. **Crypto incident SLA** – acknowledge within 2 business hours; provide root-cause analysis within 5 working days.
5. **Audit & testing rights** – organisation may perform penetration tests focused on cryptographic endpoints once per calendar year, subject to 10 days' notice.
6. **Termination for non-compliance** – failure to meet milestone dates may trigger penalty fees up to 5 % of annual contract value or early termination.

   Tip – Legal teams should store the PQC Annex as a standalone template (assets/contracts/pqc-annex.docx) to streamline procurement. All clauses reference external artefacts (CBOM spec, FAL) by version number to avoid re-negotiation when the lists update.

13.6 13.6 Technical artefacts and interfaces (300 words)

13.6.1 13.6.1 Cryptography Bill of Materials (CBOM)

A CBOM is a JSON document (CycloneDX schema `component:type="cryptography"`) listing:

- Algorithm (e.g., `rsa2048`, `ml-kem-768`)
- Protocol context (`tls1.3`, `ssh2`) and key sizes
- Certificates or key IDs, including expiry and usage (signing, encryption)
- Hardware anchoring (TPM, HSM model & firmware version)
- Compliance tags (FIPS 203, CC EAL4+)

Suppliers must sign the CBOM using DSSE (in-toto) and attach the signature envelope as `*.cbom.sig`.

13.6.2 13.6.2 SBOM-CBOM linkage

If a supplier already provides a Software Bill of Materials (SBOM), the CBOM should reference SBOM components via `bom-link` for traceability. Example snippet:

```
{
  "bom-link": "urn:uuid:123e4567-e89b-12d3-a456-426614174000",
  "algorithm": "ml-kem-768",
  "context": "tls1.3",
  "status": "hybrid"
}
```

13.6.3 13.6.3 Delivery channels

- **API** – Tier 1 suppliers push CBOMs to `/api/v1/cbom` with OAuth 2.0 MTLS.
- **S3 bucket** – Tier 2 post JSON files to `s3://cbom-uploads/<supplier>/<YYYY-MM>/`.
- **Email gateway** – Tier 3 may email CBOMs signed with PGP; files routed to an ingest Lambda.

13.6.4 13.6.4 Validation pipeline

Upon receipt, the organisation's **Crypto Intake Service** performs:

1. **Schema validation** – rejects non-conformant JSON.
2. **Signature check** – DSSE verification against supplier's root cert.
3. **Policy scan** – flag forbidden algorithms; raise ticket if found.
4. **Graph merge** – append assets to central CBOM graph database.

Failures trigger alerts to the *Supplier Risk Queue* (Jira project `SRQ`).

13.7 13.7 Supplier assessment workflow (180 words)

The following swim-lane illustrates the annual assessment for a Tier 1 supplier:

```
Supplier    Submit self-assessment (questionnaire Q-PQC-001)

Risk Team    Score questionnaire (scale 0-5)

Crypto-Sec COE    Review CBOM → run lab tests (hybrid TLS)

Procurement    Evaluate penalties/bonuses → update contract
```

Scores below 3 trigger a **Corrective Action Plan (CAP)**. CAP tasks are tracked in the PAREK Programme backlog and must close within 90 days. Sup-

pliers with sustained scores 4 across two consecutive assessments may earn incentive rebates (1 % of contract value) or preferred tender status.

13.8 13.8 Tooling ecosystem (150 words)

Function	Recommended tool / spec	Notes
CBOM authoring	`cyclonedx-python-lib`	CLI + library support
DSSE signing	`sigstore/cosign`	Leverage Fulcio CA
Validation pipeline	Custom Go microservice	Pluggable policy engine
Graph storage	Neo4j or Amazon Neptune	Supports GraphQL API
Dashboard & KPIs	Grafana + Prometheus	CBOM ingestion metrics

Integration playbooks live under `scripts/integration/` with Terraform modules for AWS and Azure, ensuring suppliers can spin up the same pipeline in their staging environments.

13.9 13.9 Governance forums (120 words)

- **Quarterly Supplier Cryptography Board (SCB)** – chaired by the CISO; Tier 1 suppliers present migration progress. Outputs: meeting minutes, updated risk register.
- **Monthly CBOM Ops Call** – operational teams review ingestion metrics, false-positive rates, upcoming schema changes.
- **Annual PQC Summit** – all suppliers invited; roadmap updates, lessons learned, and tooling demos shared. Attendance is a contract requirement for Tier 1 and 2 suppliers.

Governance artefacts are stored in SharePoint folder `Governance/Supply-Chain/` and referenced in Document Control.

13.10 13.10 Integration with PAREK KPIs (120 words)

The following metrics flow into §15:

KPI ID	Metric	Target	Data source
SC-1	% suppliers with valid CBOM	98 %	CBOM intake logs
SC-2	Mean CBOM ingestion latency	2 h	Pipeline dashboard
SC-3	% Tier 1 PQC-capable in test	100 % by 2027-Q4	Supplier roadmap
SC-4	Crypto incident SLA breach count	0 per quarter	GRC ticket system

These KPIs feed the executive dashboard and are reported to regulators under NIS-2 critical-infrastructure obligations.

13.11 13.11 Common pitfalls & mitigations (120 words)

1. **Volume overwhelm** – thousands of CBOM files per month; mitigate with batched digests and delta ingestion.
2. **Schema drift** – suppliers using outdated CycloneDX versions; mandate schema URI pinning and auto-reject mismatches.
3. **Shadow suppliers** – fourth-party components hidden inside Tier 2 deliverables; enforce SBOM-CBOM linkage and random audits.
4. **Legal bottlenecks** – protracted clause negotiations; maintain pre-approved PQC Annex template and fallback MSA language.
5. **False sense of security** – signed CBOM secure crypto; supplement with periodic binary scans and penetration tests.

13.12 13.12 Future outlook (90 words)

The EU Cyber Resilience Act may mandate **machine-readable vulnerability reporting** and real-time disclosure notices. CycloneDX 2.0 will likely promote CBOM from *extension* to *first-class object*, adding richer lifecycle metadata (retirement, key-rotation schedules). Suppliers should budget time to adopt the new schema by 2027. Quantum-safe HSM certifications (FIPS 203 level 3, CC EAL5+) are expected by 2026; contracts will update automatically when the organisation's *Approved Crypto Module List* refreshes.

13.13 13.13 References

- CycloneDX (2025). *Cryptography Bill of Materials v1.6 Specification.*
- ENISA (2024). *Threat Landscape for Supply-Chain Attacks.*
- Sigstore (2024). *Cosign 2.0 – Secure Artifact Signing.*
- European Union (2025). *Cyber Resilience Act (final text).*
- TNO (2024). *Post-Quantum Cryptography Handbook – Supplier Section.*

14 14 Roles, Responsibilities & RACI

> **Purpose of this chapter** – assign clear **R**esponsible, **A**ccountable, **C**onsulted and **I**nformed ownership for every stage, artefact and quality gate in the PAREK Framework, so that decision-making is transparent and compliant with EU governance norms (NIS 2, DORA, GDPR, CRA).

14.1 14.1 RACI legend

Code	Meaning
R	**Responsible** – executes the task / delivers the artefact
A	**Accountable** – final sign-off, owns success or failure
C	**Consulted** – provides input or subject-matter expertise
I	**Informed** – kept up to date via dashboards, reports or email

An individual or group may hold multiple codes but each task must have **exactly one Accountable (A)**.

14.2 14.2 Key organisational roles (EU context)

Abbr.	Role / body	Typical EU alignment
BoD	Board of Directors	NIS 2 Art. 20 – management oversight
CISO	Chief Information Security Officer	NIS 2 Art. 21 – technical measures
CIO	Chief Information Officer	DORA ICT strategy

Abbr.	Role / body	Typical EU alignment
CFO	Chief Financial Officer	Budget approvals, risk cost modelling
CGO	Crypto Governance Office	Operates CP-01, KMS-EU-02 policies
CRB	Crypto Review Board	Reviews new algorithms, deprecations
SCB	Supplier Cryptography Board	Oversees Tier-1 suppliers (§13)
PMO	Programme Management Office	Tracks roadmap (§10)
Squad	Migration Squad (Dev-Ops)	Executes Stage E run-books
Sup	Tier-1 Supplier Representative	Provides CBOMs, attestations

14.3 14.3 PAREK life-cycle RACI matrix

Stage / Artefact	BoD	CISO	CIO	CFO	CGO	CRB	SCB	PMO	Squad	Sup
P – Inventory	I	A	C	I	R	C	I	I	R	R
— CBOM schema & tooling	I	C	C	I	A	C	I	I	R	R
— Gap register	I	A	C	I	R	—	I	C	R	C
A – Quantum Risk Assessment	I	A	C	C	R	C	I	C	—	C
— QARS model weights	I	A	C	C	R	C	—	C	—	I
R – Road-map & Readiness	A	C	A	A	C	—	C	R	C	I
— Budget baseline	A	C	C	A	C	—	—	R	—	I
— Supplier alignment plan	I	C	C	C	C	—	A	R	—	R
E – Execution & Migration	I	A	A	I	C	C	I	C	R	R
— Pilot roll-out	I	C	A	I	C	C	I	C	R	R
— Rollback execution	I	A	A	I	—	—	I	C	R	R

Stage / Artefact	BoD	CISO	CIO	CFO	CGO	CRB	SCB	PMO	Squad	Sup
K – Key Governance & Improvement	I	A	C	C	R	A	C	I	C	C
— KPI dashboard (K-1 → K-5)	I	A	C	C	R	C	C	I	C	I
— Policy CP-01 revision	I	C	C	I	A	R	I	I	—	C
Quality gates (G1-G4)	A	A	A	C	R	C	I	R	C	I

Legend: **R = Responsible, A = Accountable, C = Consulted, I = Informed**.

14.4 14.4 Governance cadence (100 words)

Forum	Frequency	Chair	Key outputs
Steering Comm.	Quarterly	BoD	Budget, KPI review, escalations
CGO Weekly Ops	Weekly	CGO	CBOM delta report, KPI trend
CRB Algorithm	Ad hoc	CRB	Algorithm approval/deprecation
SCB Supplier	Quarterly	CISO	Supplier compliance scorecard

Outputs feed Document Control and Stage K dashboards.

14.5 14.5 EU regulatory mapping (150 words)

- **NIS 2 Art. 20** – Board is *Accountable* for cybersecurity risk management → BoD holds **A** for quality gates.
- **DORA (EU 2022/2554) Art. 12** – ICT risk management → CIO shares **A** in Stages R and E.
- **GDPR Art. 32** – Security of processing → CISO ensures encryption strength (**A** in A, E, K).
- **CRA Draft Art. 35** – Supplier obligations → SCB assigns **A** to supplier compliance artefacts.

Alignment table stored under `assets/compliance/eu-mapping.xlsx`.

14.6 14.6 Role onboarding & training (80 words)

Each role receives a tailored induction pack (OneDrive folder `Training/PAREK/<role>`), containing: - Role charter & RACI excerpt - Relevant policies (CP-01, KMS-EU-02) - Playbooks (incident response, algorithm review) - e-Learning module (SCORM) with EU regulatory quiz

Completion tracked via LMS; minimum pass score = 85 %.

15 15 KPIs & Reporting Dashboard" authors

> **Purpose of this chapter** – define the key-performance indicators (KPIs), data flows and reporting dashboards that quantify progress and operational health of the PAREK Programme. Metrics are calibrated to EU supervisory expectations under **NIS 2**, **DORA** and the forthcoming **Cyber Resilience Act (CRA)**.

15.1 15.1 Why KPIs matter (120 words)

The EU regulatory shift from *best-effort* to *demonstrable assurance* means boards must produce hard evidence that quantum-risk controls are working. KPIs convert the qualitative objectives of PAREK into quantifiable signals that:

1. **Steer execution** – highlight bottlenecks early.
2. **Inform regulators** – feed mandatory NIS 2 incident and compliance reports.
3. **Drive supplier accountability** – tie contract penalties/bonuses to measurable outcomes.

Without robust KPIs, crypto-agility devolves into one-off migrations, risking drift and audit findings.

15.2 15.2 KPI taxonomy (100 words)

KPIs are grouped into three tiers:

Tier	Audience	Frequency	Purpose
T1 – Executive	Board, regulators	Quarterly	Programme health, compliance status
T2 – Operational	CISO, CGO, PMO	Monthly	Stage-level performance, SLA breaches
T3 – Tactical	Dev-Ops squads	Daily	Deployment metrics, incident telemetry

This chapter lists core Tier 1 and Tier 2 KPIs. Tactical metrics are documented in Stage E run-books.

15.3 15.3 Core KPI catalogue (250 words)

KPI ID	Stage link	Metric (EU aligned)	Calculation / data source	Target	Alert threshold	Reg. mapping
P-1	P	CBOM coverage	`#assets with valid CBOM / #assets in scope`	98 %	<95 %	CRA Art 23
A-1	A	High-risk assets (QARS 0.65) remaining	Count from `risk_registry.csv`	$\rightarrow 0$ by 2029-Q4	$>$ Baseline trend-line	NIS 2 Art 21
R-1	R	Schedule variance	`planned finish - actual` (days)	± 0–10 days	>15 days	DORA Art 12
E-1	E	PQC handshake success rate	Envoy / Prometheus metric	99.9 %	<99.5 %	NIS CSIRT guidance
E-2	E	Median handshake latency delta	`PQC_latency - baseline_latency`	$+5$ ms	$>+10$ ms	ENISA perf. rec.
K-1	K	Unsupported algorithm instances detected	Zeek/Suricata rules	0	>0	GDPR Art 32

KPI ID	Stage link	Metric (EU aligned)	Calculation / data source	Target	Alert threshold	Reg. mapping
K-2	K	Mean Time to Remediate Crypto (MTTR-C) – high-risk	`Σ resolution time / # incidents`	30 days	> 45 days	DORA RTS
SC-1	§13	Suppliers with on-time CBOM and attestation	`#compliant / #total suppliers`	95 %	< 90 %	CRA Art 35
M-1	§10	Programme budget adherence	`actual spend / budget`	110 %	> 120 %	Board policy

15.4 15.4 Data architecture (150 words)

```
CBOM API                    Postgres (risk_registry)   Grafana API
             Lambda ETL
Zeek logs    Kafka bus

Jira API                     Prometheus (E-metrics)    Grafana API
```

- **Ingest layer** – Kafka collects CBOM deltas, Zeek alerts, deployment metrics.
- **Storage layer** – time-series in Prometheus; relational in Postgres.
- **Analytics layer** – Python notebook (`scripts/analysis/kpi_report.ipynb`) calculates monthly aggregates.
- **Visual layer** – Grafana dashboards; snapshots auto-export as PNG for board packs.

All components run in EU datacentres (GDPR Art 44 compliant). Access controls via Azure AD groups.

15.5 15.5 Dashboard design (120 words)

15.5.1 Executive dashboard

- **Gauge** – CBOM coverage (P-1)
- **Stacked bar** – High/medium/low assets over time (A-1)

- **Line** – Budget vs. actual (M-1)
- **Heat-map** – Supplier compliance (SC-1)

15.5.2 Operational dashboard

- **Table** – Unsupported algorithm findings (K-1) by business unit
- **Histogram** – MTTR-C distribution (K-2)
- **Sankey** – Incident cause → resolution path
- **Alert panel** – Live E-metrics (E-1, E-2)

Grafana JSON imports stored under `assets/grafana/kpi_dashboards/`.

15.6 15.6 Governance & review cadence (120 words)

Report	Audience	Frequency	Delivery channel	Owner
KPI snapshot (PDF)	Board	Quarterly	SharePoint / email	PMO
KPI drill-down deck	CGO	Monthly	Confluence	CGO
KPI raw export (CSV)	Regulators	Annual	SFTP to CSIRT	CISO

Each quarter, the Steering Committee reviews trend deltas. Any KPI breaching alert threshold triggers a **Corrective Action Plan (CAP)** logged in Jira.

15.7 15.7 Continuous improvement loop (100 words)

1. **Detect** – KPI alert fires.
2. **Diagnose** – Root-cause analysis meeting within 5 days.
3. **Decide** – CRB or CGO selects remediation (e.g., policy tweak, supplier escalation).
4. **Deliver** – Squad implements; KPI flagged "watch" for 30 days.
5. **Document** – Lessons-learned stored in Confluence.

KPIs themselves undergo annual review (Stage K). Weightings or new metrics added through change-control procedure CP-01-KPI-UPDATE.

15.8 15.8 EU regulatory reporting alignment (120 words)

- **NIS 2** – P-1, K-1, K-2 feed into the *Security Measures* section of the annual NIS 2 compliance report sent to the national CSIRT.

- **DORA** – K-2, E-metrics underpin the ICT Risk Management template required by ESAs.
- **CRA** – SC-1 and CBOM coverage support product security declarations.
- **ECB TIBER-EU** – A-1 trend informs the threat-intelligence baseline for red-team tests.

Mapping table maintained at `assets/compliance/kpi-eu-map.xlsx`.

15.9 15.9 Common pitfalls & mitigations (100 words)

1. **Metric overload** – focus on < 15 KPIs; archive vanity metrics.
2. **Gaming the numbers** – random audits of data sources; automated anomaly detection.
3. **Stale dashboards** – CI job fails; alert on last data-refresh timestamp > 1 day.
4. **One-size targets** – calibrate KPIs per business unit; avoid blanket thresholds.

15.10 15.10 Next steps

- Finalise Grafana dashboard JSON after Sections 8–12 baseline metrics.
- Include KPI snapshot in next Board pack (Q3 2025).
- Schedule ENISA-style KPI workshop for suppliers (Q4 2025).

15.11 15.11 References

1. ENISA (2024). *Guidelines on KPIs for Cybersecurity Measures.*
2. European Commission (2023). *NIS 2 Directive.*
3. European Parliament (2025). *Cyber Resilience Act – Final Text.*
4. EBA (2024). *ICT Risk Management under DORA.*
5. Grafana Labs (2025). *Best Practices for KPI Dashboards.*

16 16 Reference Architectures & Tooling

Purpose of this chapter – provide opinionated, EU-aligned reference architectures that engineering teams can adopt or adapt when implementing PAREK migrations. Each pattern embraces open-source baselines, indicates where commercial substitutes may

slot in, and highlights regulatory hooks (NIS 2, DORA, CRA, eIDAS 2).

16.1 16.1 Reading guide (80 words)

Each subsection presents:

1. **Context** – why the pattern matters.
2. **Diagram** – ASCII or UML sketch.
3. **Component list** – open-source baseline + commercial alternatives.
4. **EU compliance notes** – which articles/standards the pattern satisfies.
5. **Implementation tips** – common pitfalls, performance notes.

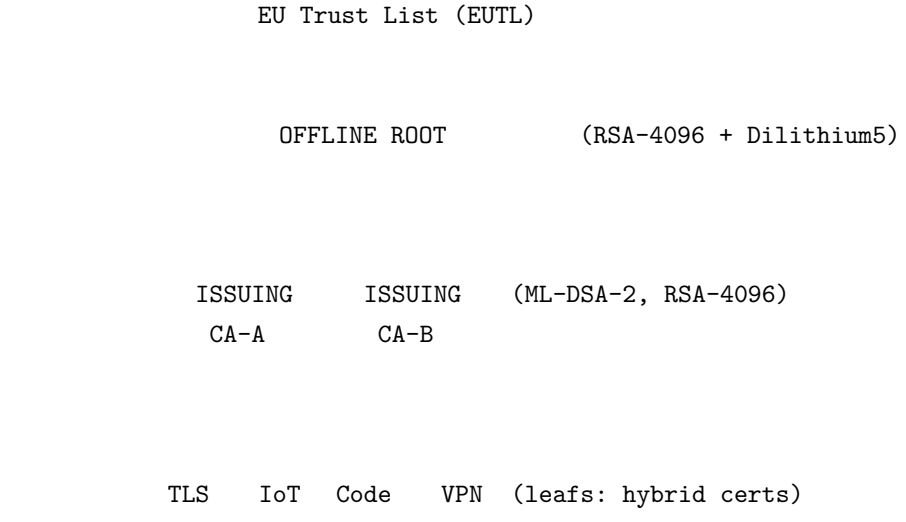
Full Terraform or Helm charts live in `assets/infra/`.

16.2 16.2 PQ-ready PKI (*Pattern RA-PKI-EU*)

16.2.1 16.2.1 Context

Most TLS, code-signing and device-auth chains depend on a X.509 hierarchy. Upgrading to hybrid or PQ-only certificates without forklift replacements requires a crypto-agile PKI.

16.2.2 16.2.2 Diagram



16.2.3 16.2.3 Components

Function	Open-source	Commercial
CA core	EJBCA CE	Entrust PKIaaS EU
HSM	SoftHSM + PKCS#11	Thales Luna HSM7 (EU datacentre)
ACME	`certbot` (OQS-patched)	Sectigo Certificate Manager

16.2.4 16.2.4 EU compliance

- **eIDAS 2** QES requirements → Offline root must be hosted in EU + QTSP audit.
- **NIS 2 Art. 21** technical controls → dual control on root key ceremonies.

16.2.5 16.2.5 Implementation tips

- Use **nested signatures**: RSA-4096 outer, Dilithium5 inner to satisfy legacy clients.
- Test OCSP responders for 4 kB cert sizes.

16.3 16.3 Hybrid TLS termination (*RA-TLS-HYB*)

16.3.1 Context

Web/API gateways must negotiate Kyber + X25519 KEM yet preserve performance.

16.3.2 Diagram

```
Users  Cloudflare Zaraz (TLS 1.3)  Envoy Edge  Service Mesh  App Pods
         Kyber768+X25519          Kyber768+X25519    mTLS (OQS-gRPC)
```

16.3.3 Components

Layer	OSS baseline	Commercial EU-hosted
CDN	Cloudflare beta PQC edge	Akamai Secure Edge PQC
Proxy	Envoy 1.31 + OQS-BoringSSL	NGINX Plus FIPS-PQC module
mTLS	OQS-gRPC	Istio with Thales DataShield

16.3.4 EU notes

- CRA requires "state-of-the-art" crypto → hybrid by 2026 meets "state-of-the-art" definition.
- GDPR Art. 32 encryption → document cipher suite in RoPA.

16.3.5 Tips

- Enable **GREASE** support to avoid middlebox drops.
- Capture baseline latency; expect +2-5 ms at 1 kB handshake growth.

16.4 16.4 Secure code-signing pipeline (*RA-CODE-SIGN*)

16.4.1 Diagram

```
Git Commit  CI Build  Cosign Sign (Dilithium2)  Rekor Transparency Log  Artifactory
```

16.4.2 Components

Step	Tool (OSS)	Alt (Commercial)
Sign	`sigstore/cosign --key dilithium.key`	Venafi CodeSign Protect
Log	`sigstore/rekor` EU cluster	Ledger EU Notary
Verify	`cosign verify --key dilithium.pub`	Jenkins PQC plugin

16.4.3 EU alignment

- CRA mandates SBOM/CVEs disclosure → attach CBOM + SBOM via Sigstore DSSE.
- DORA ICT - data integrity → use Transparency Log proofs.

16.5 16.5 CBOM ingestion & graph (*RA-CBOM-EU*)

16.5.1 Diagram

```
Supplier CBOM JSON  API Gateway (OAuth)  Kafka topic `cbom.raw`

              error queue

            ETL (Rust Lambda)  Neo4j GraphDB  Grafana Dash
```

16.5.2 Components

Function	OSS	Commercial
Gateway	Kong Gateway	Azure APIM EU
Queue	Kafka	AWS MSK (eu-west-1)
Graph	Neo4j Community	Amazon Neptune

16.5.3 EU notes

- Store all supplier data within EEA to satisfy GDPR Art. 44.

16.6 16.6 Crypto-agile secret management (*RA-SECRETS*)

16.6.1 Diagram

```
Apps  HashiCorp Vault (Transit Engine PQC plugin)  HSM partition (ML-KEM)
```

16.6.2 Implementation tips

- Use **Key Versioning** to rotate to future algorithms (e.g., ML-KEM-1024).
- Enable **Key Type Tags** to block RSA key generation post-2030.

16.7 16.7 Mapping architectures to PAREK stages

Stage	Primary reference pattern	Artefacts produced
P	RA-CBOM-EU	CBOM graph export
A	(N/A) – consumes CBOM	Risk registry
R	Integration of RA-PKI-EU	Roadmap epics
E	RA-TLS-HYB, RA-CODE-SIGN	Run-books, metrics
K	RA-SECRETS, monitoring stack	KPI dashboards

16.8 16.8 EU compliance cross-reference (summary)

Pattern	NIS 2	DORA	CRA	eIDAS 2	GDPR
RA-PKI-EU		—	—		—
RA-TLS-HYB				—	

Pattern	NIS 2	DORA	CRA	eIDAS 2	GDPR
RA-CODE-SIGN					—
RA-CBOM-EU				—	
RA-SECRETS			—	—	

Full mapping sheet lives in `assets/compliance/patterns-eu-matrix.xlsx`.

16.9 16.9 Next steps

- Pilot **RA-TLS-HYB** on staging APIs (Q4 2025).
- Migrate code-signing pipeline to Dilithium2 by Q1 2026.
- Integrate CBOM graph with risk dashboard (Stage K KPI P-1) before next NIS 2 audit.

16.10 16.10 References

1. ETSI (2024). *TS 119 996 – Algorithm Agility Principles.*
2. Sigstore (2025). *PQC Roadmap.*
3. ENISA (2025). *Architecture Patterns for Post-Quantum Migration.*
4. Cloudflare (2025). *Hybrid KEM Performance Whitepaper.*
5. CEN/CENELEC (2025). *Guideline on PQC-Ready PKIs.*

17 17 Glossary & Acronyms (CEN/CENELEC & ISO-aligned)

Purpose – harmonise terminology across the handbook and supplier communications. Definitions derive, where possible, from authoritative European standards: **CEN/CENELEC Guide 30:2015** (*European Standardisation – Vocabulary*), **EN ISO/IEC 2382** (*Information technology – Vocabulary*) and **ETSI TR 103 684** (*Algorithm Agility and Post-Quantum Cryptography*). Where no official wording exists, the editorial team supplies a consensual definition.

Abbreviations are ordered alphabetically; initialisms are uppercase, terms are in Title Case.

Term / Acronym	Definition (EU standard reference)
AES – Advanced Encryption Standard	Symmetric block cipher standardised in ISO/IEC 18033-3.
Algorithm Agility	Ability of a system to support, select and switch between multiple cryptographic algorithms with minimal impact (ETSI TR 103 684).
CBOM – Cryptography Bill of Materials	Machine-readable inventory of algorithms, keys, certificates and crypto modules contained in a product; extension to CycloneDX v1.6 (CEN/CENELEC draft prEN 17720).
CEN – Comité Européen de Normalisation	European Committee for Standardization responsible for non-electrotechnical standards.
CENELEC – Comité Européen de Normalisation Électrotechnique	European Committee for Electrotechnical Standardization.
CRQC – Cryptographically Relevant Quantum Computer	Quantum computer capable of performing Shor-style attacks on RSA/ECC keys of practical length (EN ISO/IEC 2382-37 draft).
CRA – Cyber Resilience Act	EU regulation proposal on cyber-secured products (COM/2022/454).
CVSS – Common Vulnerability Scoring System	Industry standard for rating IT vulnerabilities (ISO/IEC 30111).
Dilithium	Lattice-based digital-signature scheme selected by NIST for standardisation (FIPS 204).
DORA – Digital Operational Resilience Act	EU regulation 2022/2554 on ICT risk management for the financial sector.
DSSE – Delegated Supply-chain Signing Envelope	JSON envelope format binding artefact digests and signature metadata (IETF draft).

Term / Acronym	Definition (EU standard reference)
ENISA – European Union Agency for Cybersecurity	EU agency providing guidance on cybersecurity and cryptography.
eIDAS 2	Regulation (EU) 2024/126 on digital identity and trust services.
ETSI – European Telecommunications Standards Institute	Standards body producing ICT technical specs (e.g., ETSI TS 119 996 on algorithm agility).
FAL – Forbidden Algorithm List	Organisational list banning weak or deprecated algorithms (internal policy; reference CRA Art 23).
FIPS – Federal Information Processing Standard	U.S. Government cryptography standards (e.g., FIPS 203 ML-KEM).
HNDL – Harvest-Now-Decrypt-Later	Attack model where adversary stores encrypted data today to decrypt after CRQC becomes available (CEN/CENELEC use case).
HSM – Hardware Security Module	Physical device safeguarding cryptographic keys and operations (ISO/IEC 19790).
Hybrid Key Exchange	Protocol combining classical and post-quantum Key Encapsulation Mechanisms (KEMs) to derive a shared secret (IETF RFC 9399).
ISO – International Organization for Standardization	Global standardisation body collaborating with IEC on IT.
Key Governance	Processes and controls ensuring lifecycle management of cryptographic keys (EN ISO/IEC 27002:2022, 10.10).
Kyber / ML-KEM	Module-lattice KEM selected by NIST (FIPS 203).
MTTR-C – Mean Time to Remediate Crypto	Average time to replace or fix weak cryptography after detection (DORA ICT RTS draft).
NIS 2	Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union.

Term / Acronym	Definition (EU standard reference)
OCSP – Online Certificate Status Protocol	Internet X.509 revocation protocol (IETF RFC 6960).
PAREK	Five-stage EU PQC transition framework: **P**-Inventory, **A**-Risk Assessment, **R**-Road-mapping, **E**-Execution, **K**-Governance.
PQC – Post-Quantum Cryptography	Cryptographic primitives believed secure against quantum adversaries (ISO/IEC 2382-37 draft term).
QACKER – Quantum Hacker	Community-driven portal tracking quantum exploits and proof-of-concept attacks on classical cryptography (https://www.qacker.com).
QARS – Quantum-Adjusted Risk Score	Composite metric weighting shelf-life, migration effort and threat horizon.
QTSP – Qualified Trust Service Provider	Entity providing qualified trust services under eIDAS 2.
RSA	Public-key cryptosystem based on integer factorisation (ISO/IEC 14888-2).
SBOM – Software Bill of Materials	List of software components in a product (ISO/IEC 5962:2021 – SPDX).
SCB – Supplier Cryptography Board	Governance forum reviewing supplier PQC readiness (§13).
Shor's Algorithm	Quantum algorithm for factoring and discrete logarithms (ISO/IEC 2382-37 ref).
SPHINCS+	Stateless hash-based signature scheme selected by NIST (FIPS 205).
TLS 1.3	Transport Layer Security protocol version 1.3 (IETF RFC 8446).
X.509 Certificate	Public-key certificate standard (ITU-T X.509; also ISO/IEC 9594-8).

17.1 Notes on usage

- Where CEN/CENELEC or ISO vocabulary provides an exact wording, that phrasing is preferred verbatim.
- Internal policy acronyms (e.g., QARS, SCB) are capitalised to signal organisational scope.
- Terms introduced by NIST but not yet in ISO (e.g., ML-KEM) keep NIST naming with cross-reference to pending ISO work items.

18 18 Templates, Check-lists & Sample Artefacts

Purpose – catalogue the ready-to-use artefacts that accelerate PAREK implementation: spreadsheets, questionnaires, run-books and document stubs. All templates live under the repository's `assets/templates/` folder so teams can clone or download them directly.

The table lists each template, its intended use, recommended format and repository path.

#	Template name	Purpose	Format	Repo path
1	**CBOM JSON Schema**	Validate supplier cryptography bills of materials against CycloneDX extension	`.json`	`assets/templates/cbom-schema/pqcbom-1.6.json`

#	Template name	Purpose	Format	Repo path
2	**Asset Inventory Spreadsheet**	Manual fallback sheet for systems where automated scanning is not feasible	`.xlsx`	`assets/templates/inventory/inventory-bas`
3	**Risk Calculator Notebook**	Jupyter notebook implementing QARS formula with sample data	`.ipynb`	`assets/templates/risk/qars_calc.ipynb`
4	**Supplier Questionnaire (Q-PQC-001)**	Collect vendor crypto posture & roadmap (Tier 1/2)	`.docx`	`assets/templates/supplier/q-pqc-001.doc`
5	**PQC Contract Annex**	Standard legal clause bundle (CRA-ready)	`.docx`	`assets/templates/contracts/pqc-annex.do`
6	**Migration Run-book Stub**	Markdown skeleton for Stage E deployments	`.md`	`assets/templates/execution/migration_ru`
7	**Rollback Playbook**	Script + checklist for emergency cipher rollback	`.sh` + `.md`	`assets/templates/execution/rollback/`

#	Template name	Purpose	Format	Repo path
8	**KPI Dashboard JSON**	Grafana import for executive KPI panel	`.json`	`assets/templates/kpi/kpi_dashboard.json`
9	**Incident Report Form (ENISA style)**	72-hour notification template for NIS 2 major incidents	`.docx`	`assets/templates/incidents/nis2_incident`
10	**Lessons-Learned Retrospective Deck**	Slide deck for post-migration review meetings	`.pptx`	`assets/templates/lessons/retro_template`

18.0.1 How to use

1. **Download or clone** the required file from the path above.
2. **Fill in the yellow-highlighted fields** – those are mandatory for audit.
3. **Version-control** completed artefacts in your project folder (`/project/<work-package>/docs/`).
4. **Submit** via pull request or the SharePoint drop-off library as instructed in §10 or §12.

18.0.2 Planned additions *(placeholder)*

Template	ETA	Owner
KPI auto-emailer script	Q1 2026	CGO-DevOps
CBOM→Neo4j import Lambda	Q2 2026	DevOps-Infra

19 19 Appendices – Supporting Artefacts & Deep-Dive Material

Purpose – enumerate and briefly describe the supplementary artefacts that provide extra depth, raw data or worked examples refer-

enced throughout the handbook. Each appendix lives either as a standalone Markdown/PDF in `assets/appendix/` or as an embedded section below.

19.1 Suggested Appendix Catalogue

ID	Working Title	Intended Content (summary)	Format & Location
A	Algorithm & Parameter Cheat-Sheets	One-page tables for ML-KEM, ML-DSA, SPHINCS+ parameters (security level, key sizes, cipher-suite IDs). Useful for architects and auditors.	`assets/appendix/A-algo-cheatsheet.pdf`
B	CRQC Scenario Planning Worksheets	Excel model pre-loaded with Fast/Baseline/Delayed threat horizons (§9.7) and Monte Carlo templates for budget impacts.	`assets/appendix/B-scenario-worksheets.xlsx`
C	EU Regulatory Mapping Matrix	Pivot table mapping handbook sections, KPIs and reference architectures to NIS 2, DORA, CRA, eIDAS 2 articles.	`assets/appendix/C-eu-reg-matrix.xlsx`

ID	Working Title	Intended Content (summary)	Format & Location
D	Sample CBOM & Validation Report	Example Tier-1 supplier CBOM JSON, DSSE signature, and automated validation output.	`assets/appendix/D-sample-cbom/`
E	Q-PQC-001 Supplier Questionnaire	Blank and filled-in versions demonstrating expected depth of answers.	`assets/appendix/E-supplier-questionnaire.docx`
F	KPI Dictionary	Extended definitions, formulas and SQL/Grafana queries for every KPI in §15.	`assets/appendix/F-kpi-dictionary.md`
G	Risk Formula Reference	Derivation of QARS weights, academic citations, sensitivity analysis plots.	`assets/appendix/G-qars-formula.pdf`
H	Contract Annex Boilerplate	Full text of the PQC Annex with tracked-changes commentary and CRA cross-references.	`assets/appendix/H-pqc-annex.docx`
I	Training Matrix & Syllabi	Detailed curricula, slide decks and lab guides for Dev-Ops, IT Ops and Risk roles.	`assets/appendix/I-training-matrix/`

ID	Working Title	Intended Content (summary)	Format & Location
J	Tool Installation Scripts	Bash/PowerShell scripts to deploy reference stack (OQS-OpenSSL, Envoy, Neo4j).	`assets/appendix/J-tool-scripts/`

Feel free to re-letter or reorder appendices as the handbook matures; maintain unique IDs for citation stability.

19.2 Next-step actions

1. **Content owners** – populate each appendix folder/file before handbook v1.0 freeze (target Q1 2026).
2. **Editorial review** – ensure consistency with glossary and policy stack.
3. **Linking** – update in-text references (e.g., "see Appendix C") as each appendix finalises.

This document was generated using the PAREK open framework.