Ready for the Quantum Threat

From discovery to a fully managed certificate lifecycle

Jan Krob, TRASK Solutions
Jakub Morávek, OmniTrust

13 – 15 October 2026

ISACA
Czech Republic Chapter

Six questions, one managed path to quantum readiness

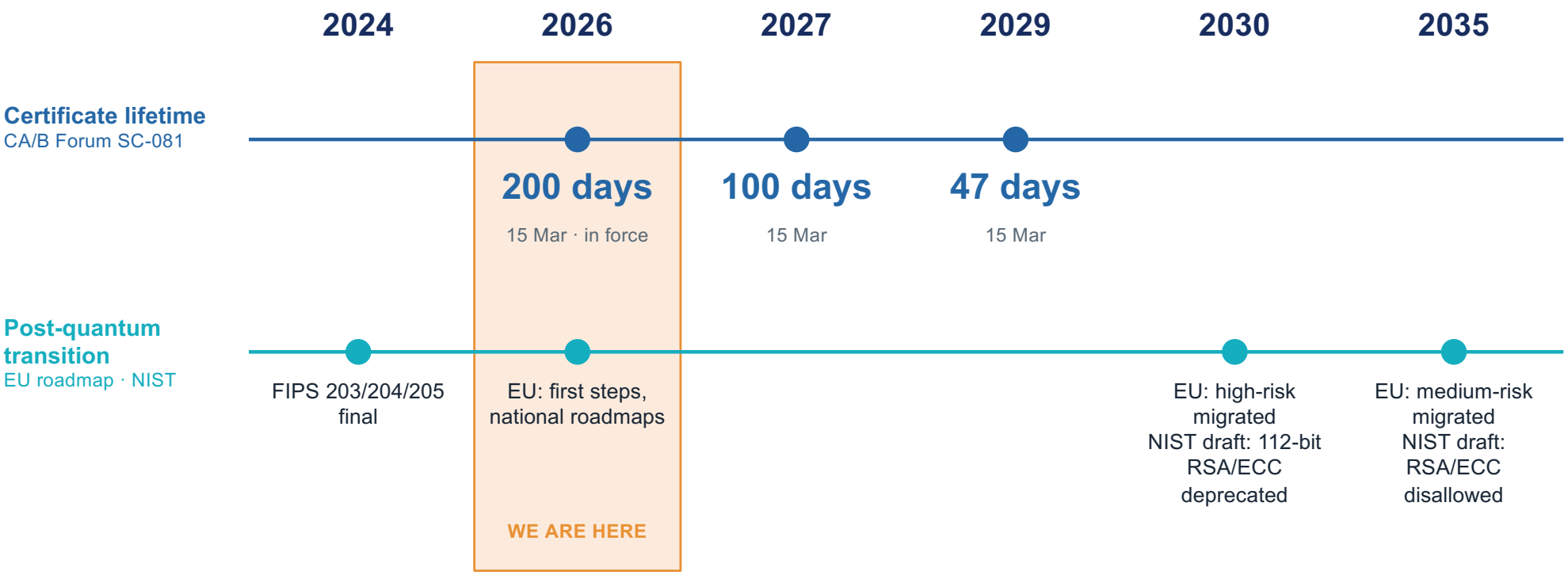
For each question, what to do and how to measure progress.

01	02	03	04	05	06
WHY?	WHEN?	WHAT?	WHERE?	WHO?	HOW?

ISACA Czech Republic Chapter

Two clocks are ticking

Q-Day is uncertain. Certificate lifetimes are not.



ISACA Czech Republic Chapter

One problem, three worlds

Each world has its own pace, risk and owner. Both clocks hit them differently.

External — WEEKS

Internet & mobile banking, open APIs, partner portals

SC-081

Direct hit: 100 → 47 days

PQC

First in line: highest exposure

Legacy — YEARS

Core systems, middleware, appliances

SC-081

Indirect: private CAs, manual renewal

PQC

Hardest: vendor-dependent

DevOps & AI — MINUTES

Kubernetes, CI/CD, microservices, AI agents and model APIs

SC-081

Already short-lived, AI even shorter

PQC

Easiest if policy-driven, AI adds volume

ISACA Czech Republic Chapter

Already required, and Q-Day is getting closer

Nobody knows the date. Regulators and research are not waiting for it.

REQUIRED AND EXPECTED

1. **EU PQC Roadmap (2025)**
   Inventory and first steps by end of 2026
2. **DORA RTS 2024/1774 Art. 6(4)**
   Change cryptography as cryptanalysis evolves
3. **DORA RTS Art. 7(4)–(5)**
   Certificate register, prompt renewal
4. **CZ Act 264/2025 + NÚKIB v4.1**
   RSA only from 3072 bits

Q-DAY OUTLOOK

28–49%

Expert odds of a quantum computer breaking RSA-2048 within 10 years. Within 15 years 51–70%.

Global Risk Institute, Quantum Threat Timeline Report 2025

Qubits needed to break RSA-2048 (log scale)



Today's estimate is ~100,000 physical qubits and about 10 days.

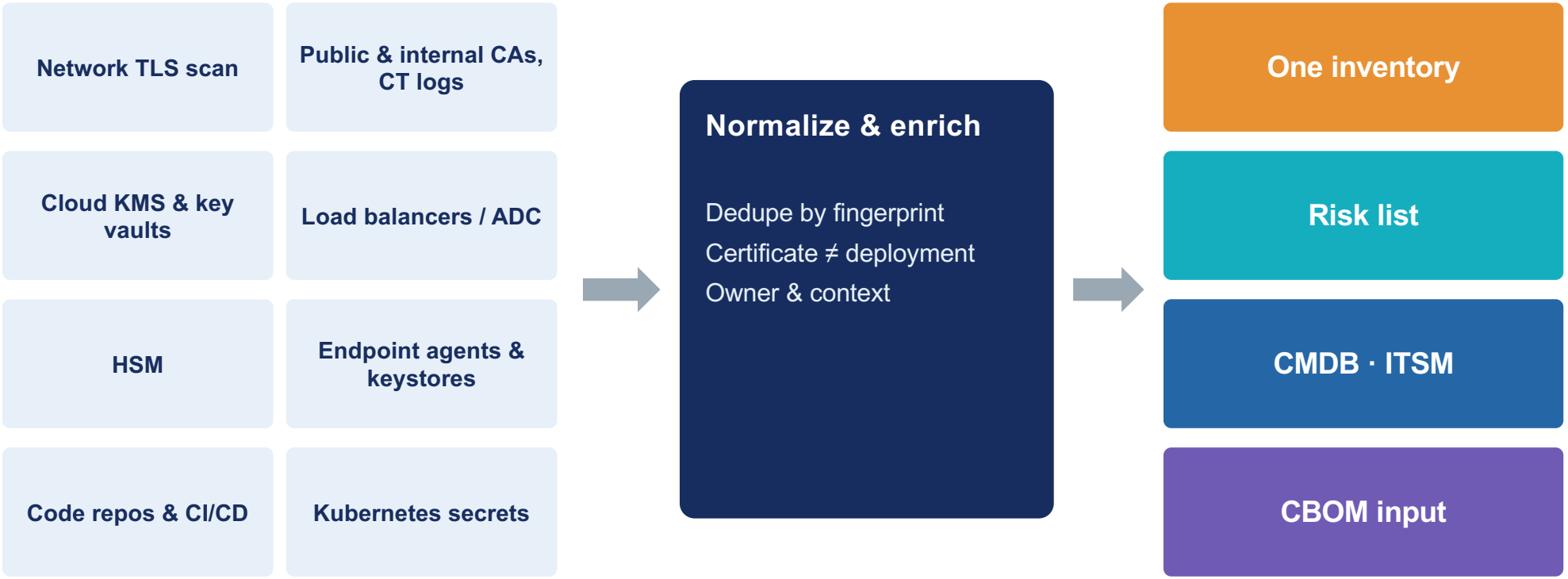
Largest machines today hold ~6,100 atom qubits, fault-tolerant operations on ~500.

Plan for the deadlines you know, not for the date nobody knows.

ISACA Czech Republic Chapter

One scanner is not enough

Many sources, one normalized inventory with owners and context.



ISACA Czech Republic Chapter

What discovery finds first

Five findings that show up in almost every first discovery.

	FINDING	WHAT WE SEE	WHY IT MATTERS
1	**Default certificates**	Vendor certificates on server management interfaces, appliances and network devices.	**Admin access protected by a key nobody controls**
2	**Self-signed fallback**	Services fall back to a self-signed certificate when the real one is missing or expired.	**Users and clients learn to ignore warnings**
3	**TLS on database ports**	Databases and middleware with their own, manually installed certificates.	**No renewal process, outage on expiry**
4	**Unknown internal CA**	An issuing CA run by one team, with no policy and no owner in the PKI team.	**Shadow PKI without revocation or audit trail**
5	**Out-of-policy crypto**	RSA-2048 below NÚKIB v4.1, SHA-1 signatures, sometimes even RSA-1024.	**Compliance gap today, PQC gap tomorrow**

ISACA Czech Republic Chapter

From inventory to risk analysis

WHY? WHEN? **WHAT?** **WHERE?** WHO? HOW?

Enrich every asset with attributes you can score – not just scan data.

Owner & CI	CMDB
Business criticality	Service · process · DORA critical function
Asset criticality	CIA rating · regulated scope
Data lifetime	How long it must stay confidential
Threat type	HNDL or TNFL
Attack vectors	Internet · partner · insider · supply chain
Crypto profile	Algorithm · key · CA
Changeability	Automated · manual · vendor

→ **Likelihood**
exposure + attack vectors

→ **Impact**
business criticality + asset criticality + data lifetime + threat type

→ **Time to change**
changeability

ISACA Czech Republic Chapter

Every asset has an owner – a role

Operational answers to the governance questions from the previous talk.

Role	Accountable for	Evidence
Crypto owner (CISO)	Algorithm policy, profiles, CA strategy	Approved policy, profile versions
Application owner	Record accuracy, renewal, testing	Owner validation, changes
PKI / platform team	CA & CLM operations, automation	Logs, SLA
Risk & compliance	Exceptions, risk acceptance	Exception register with end date
Procurement	PQC clauses in contracts and RFPs	Clauses, vendor questionnaires

PQC readiness is bought, not retrofitted

Ask for evidence in the RFP. Turn promises into obligations in the contract.

ASK AND VERIFY IN THE RFP

1. **Dated PQC roadmap**
   ML-KEM, ML-DSA and hybrid TLS by version and date
2. **Configurable cryptography**
   No hard-coded algorithms. Meets our policy and NÚKIB v4.1
3. **Automated certificate exchange**
   ACME, EST, SCEP or API. Ready for 47-day lifetimes
4. **Customer-controlled trust**
   Replace the CA and trust store without a service visit
5. **Crypto transparency**
   CBOM with algorithms, libraries and versions

Verify in the PoC, not in the questionnaire.

BIND IN THE CONTRACT

1. **Roadmap dates as obligations**
   Contract milestones, not marketing slides
2. **Fix time for crypto flaws**
   Agreed deadline for weak or broken algorithms
3. **Remedy if a date slips**
   Dated exception, service credit or exit right
4. **Same terms for subcontractors**
   Flow-down along the supply chain (DORA Art. 28, 30)

A clause today costs less than a change request later.

ISACA Czech Republic Chapter

No automation, no PQC

PQC replaces every quantum-vulnerable certificate at least once. Who does that work?

MANUAL

PQC = one project per application

Tickets, change windows, owners to chase

AUTOMATED

PQC = one policy change

From 2029 the whole public estate turns over within 47 days

WHAT AUTOMATION PAYS BACK TODAY

1. **Lower IT operations cost**
   Renewal effort moves from people to the pipeline
2. **Fewer manual errors**
   No wrong chain, wrong key or forgotten deployment
3. **No expiry outages**
   Renewed before expiry, every time (DORA RTS Art. 7(5))
4. **Audit evidence by default**
   Who, which profile, which CA, where, per certificate
5. **Faster delivery**
   Certificates in minutes instead of days
6. **Fast incident response**
   Replace a compromised CA or algorithm at pipeline speed

Automation pays for itself today and delivers PQC tomorrow.

ISACA Czech Republic Chapter

PQC migration is a business challenge first

WHY? WHEN? WHAT? WHERE? WHO? **HOW?**

CHALLENGE	WHO FEELS IT: Business	IT	Security	Risk	Audit	WHAT ADDRESSES IT
Vendors aren't ready No PQC roadmap, no date, no price	●	●	○	○	○	PQC clauses in RFPs, dated exceptions
PQC means a system upgrade Hardware, firmware and libraries, not just certificates	●	●	○			Cost model from the inventory
Changes ignore the lifecycle Off-cycle upgrades break the budget	●	○		○		Migrate at renewal, retire before 2030
Big bang temptation One deadline, everything at once	○	●		●		Waves and canary, see next slide
Rules keep moving Standards and regulators still evolving			●	○	●	Crypto-agile policy, no hard-coding
Legacy that breaks Old clients, devices and middleboxes		●	○		○	Test, proxy, isolate or retire

● feels it most ○ also affected

ISACA Czech Republic Chapter

No big bang, no cost creep

Ride the lifecycle, standardize the patterns, keep the options open.

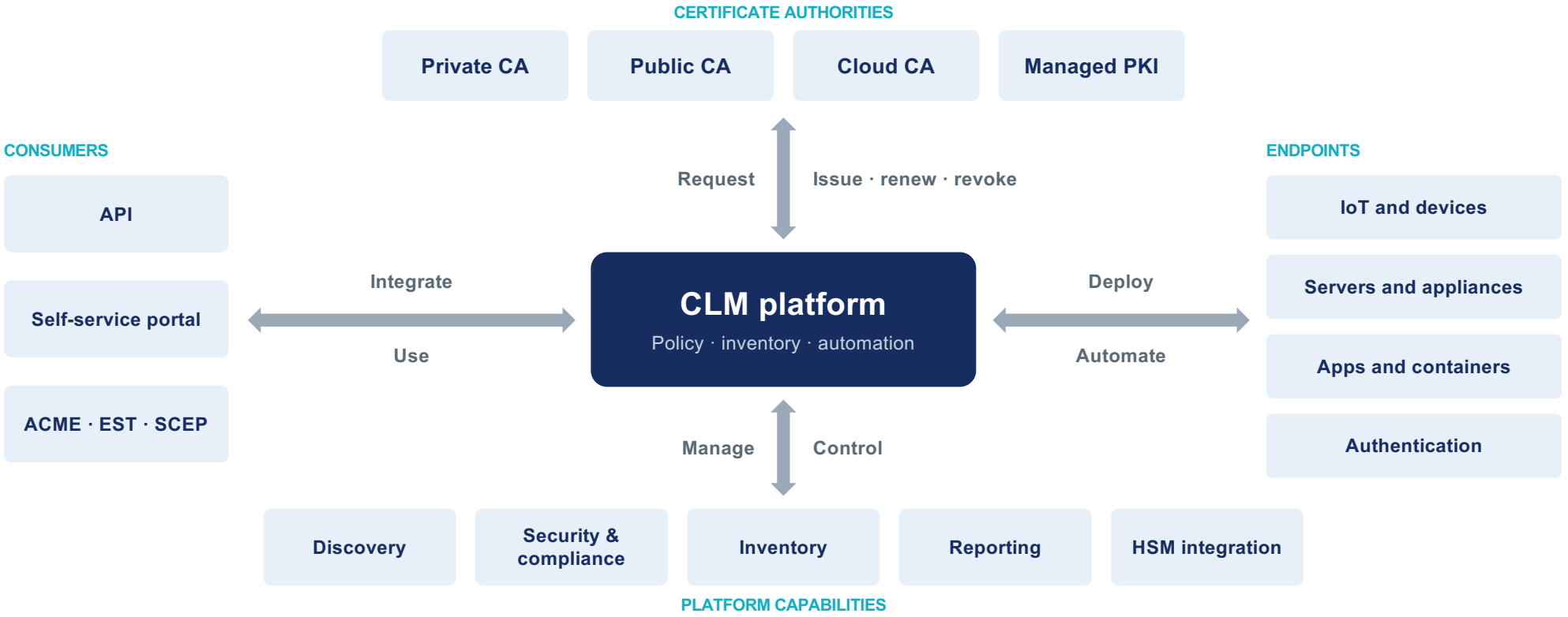
1	**Waves by priority**	Start where exposure and data lifetime are highest, one world at a time. External first.
2	**Canary first**	Roll a new profile to a small share of traffic. Watch errors, then scale up.
3	**Rollback = previous profile**	If clients fail, the platform reissues on the last working profile. No war room.
4	**Performance tests**	Bigger keys and signatures change handshake time, MTU and CPU load. Measure first.
5	**Retire, don’t migrate**	Systems leaving before 2030 get isolation and a dated exception, not a project.

Run it as a programme. Map the dependencies, be ready for delays.

ISACA Czech Republic Chapter

One platform, any CA, every endpoint

Any CA above, any consumer and endpoint around it, one policy in the middle.



ISACA Czech Republic Chapter

Policy decides, the platform executes

WHY? WHEN? WHAT? WHERE? WHO? **HOW?**

Change a profile once – re-issue at pipeline speed.



DEPLOYMENT CHANNELS

ACME	EST · SCEP · CMP	REST API	Connectors	ITSM workflow
Web servers, Kubernetes	Devices, MDM, switches	Internal platforms, CI/CD	Load balancers, key vaults	Where nothing else fits

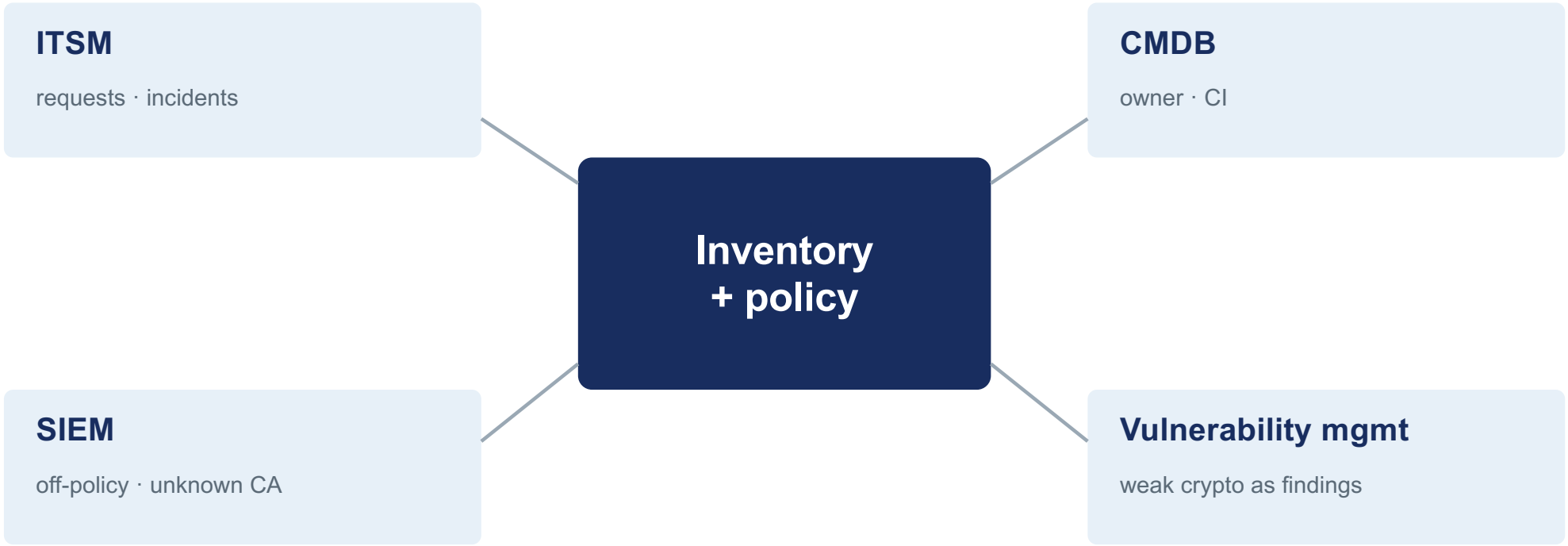
People handle exceptions and compatibility tests, not routine renewals.

ISACA Czech Republic Chapter

Stop the chaos from coming back

WHY? WHEN? WHAT? WHERE? WHO? HOW?

Continuous discovery, policy at issuance, self-service faster than the workaround.



ISACA Czech Republic Chapter

Crypto-agility is tested, not declared

A pragmatic path – value in months, measured from day one.



Weeks 0–6
% estate visible

Months 1–3
% with owner

Months 3–9
% renewals automated

Ongoing
% crypto inventory

ANNUAL DRILL

How many days to replace every certificate from CA X – or algorithm Y – in critical services?

REFERENCE · LARGE CZECH BANK

Tens of thousands of certificates
Tens of DevOps teams
Under a year to full operation
Days → minutes per certificate

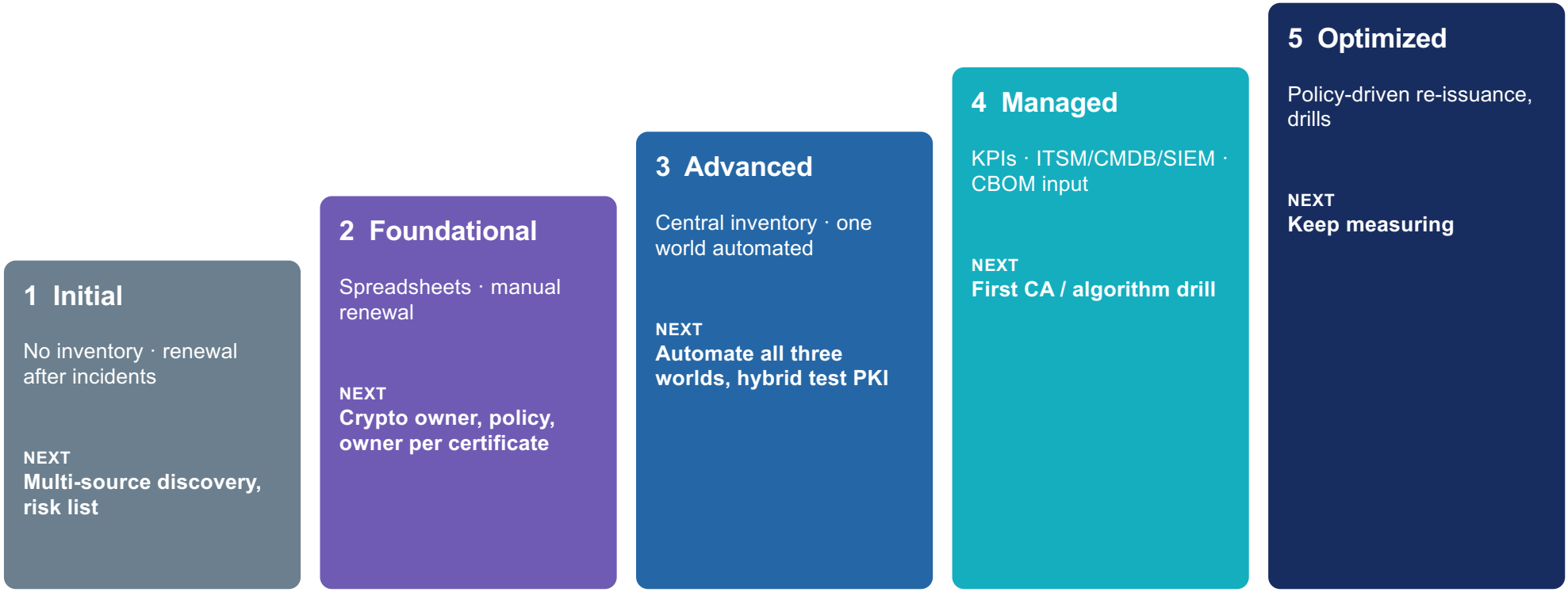
ISACA Czech Republic Chapter

Where are you today? Take one step up

WHY? WHEN? WHAT? WHERE? WHO? HOW?

WHERE TO START

Adapted from the PKI Consortium PKI Maturity Model and its PQC Readiness Extension (draft).



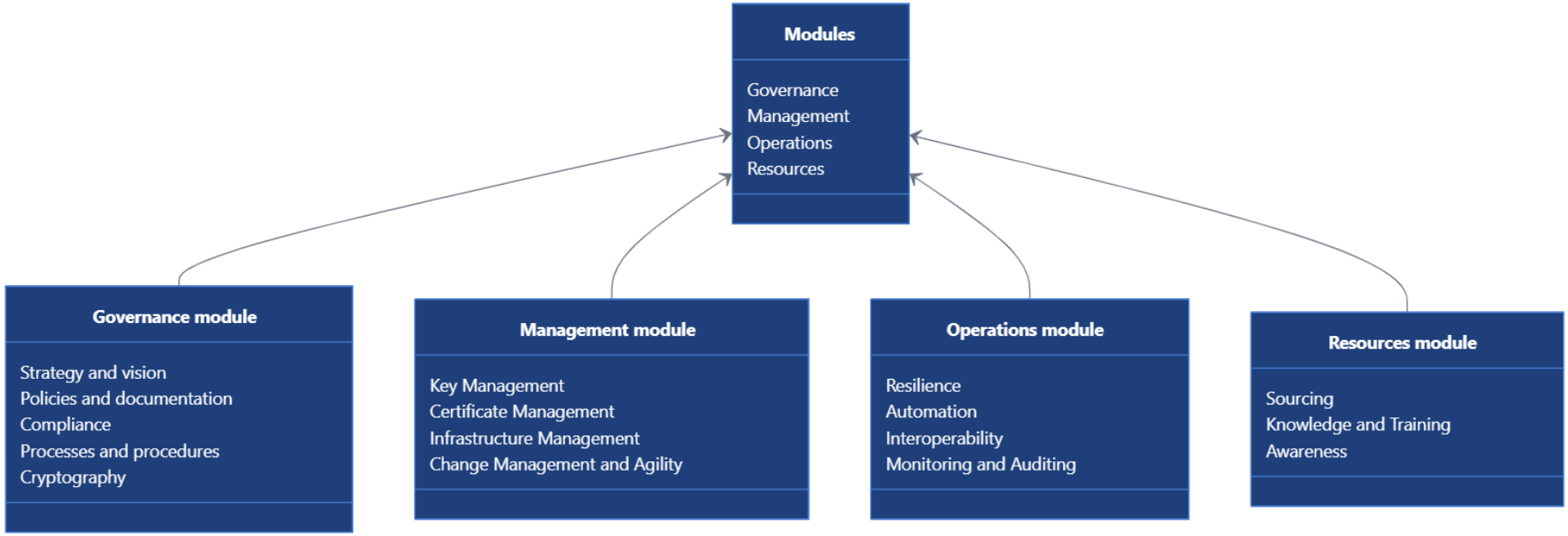
Free online self-assessment at pkic.org/wg/pkimm/assessment

ISACA Czech Republic Chapter

PKI Maturity Model with PQC extension

WHY? WHEN? WHAT? WHERE? WHO? HOW?

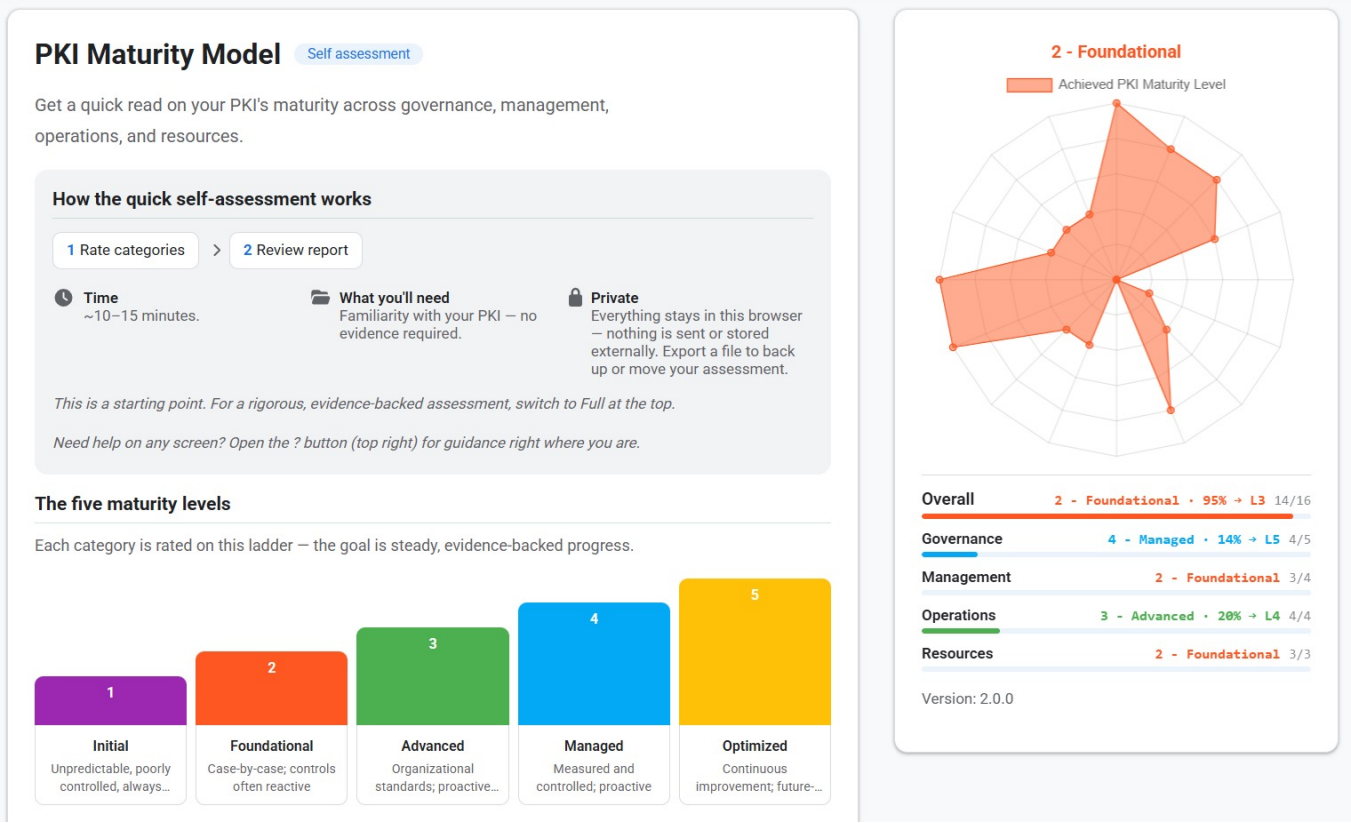
The Post-Quantum Cryptography (PQC) Readiness Extension adds quantum-safe transition criteria to the PKI Maturity Model. It introduces an extension-specific maturity signal alongside the baseline PKI MM categories, plus weight overlays that emphasize requirements most relevant to PQC migration.



ISACA Czech Republic Chapter

PKI Maturity Model

WHY? WHEN? WHAT? WHERE? WHO? HOW?



ISACA Czech Republic Chapter

Thank you. Questions?

Jan Krob, TRASK Solutions
Jakub Morávek, OmniTrust

ISACA
Czech Republic Chapter