Roadmap to Post-Quantum Migration

NISDUC Luxembourg, 06/04/2025

Nicolas Lempereur, BIPT

Institut belge des services postaux et des télécommunications

ibpt

Agenda

1. Introduction
2. PQC : solutions
3. Migration & roadmap
4. Regulators and autorities

Cryptography in modern companies…

Data confidentiality

Authentication and access control

Data integrity

Secure communication

Digital signatures

Threat scenarios

STORE-NOW & DECRYPT LATER

LONG MIGRATION PERIOD

How to deal with a threat that hasn’t yet emerged

We need preparation, awareness and planning

Well prepared company

- Migrate in Time
- Protect what really matters
- Integrate quantum-safe solutions

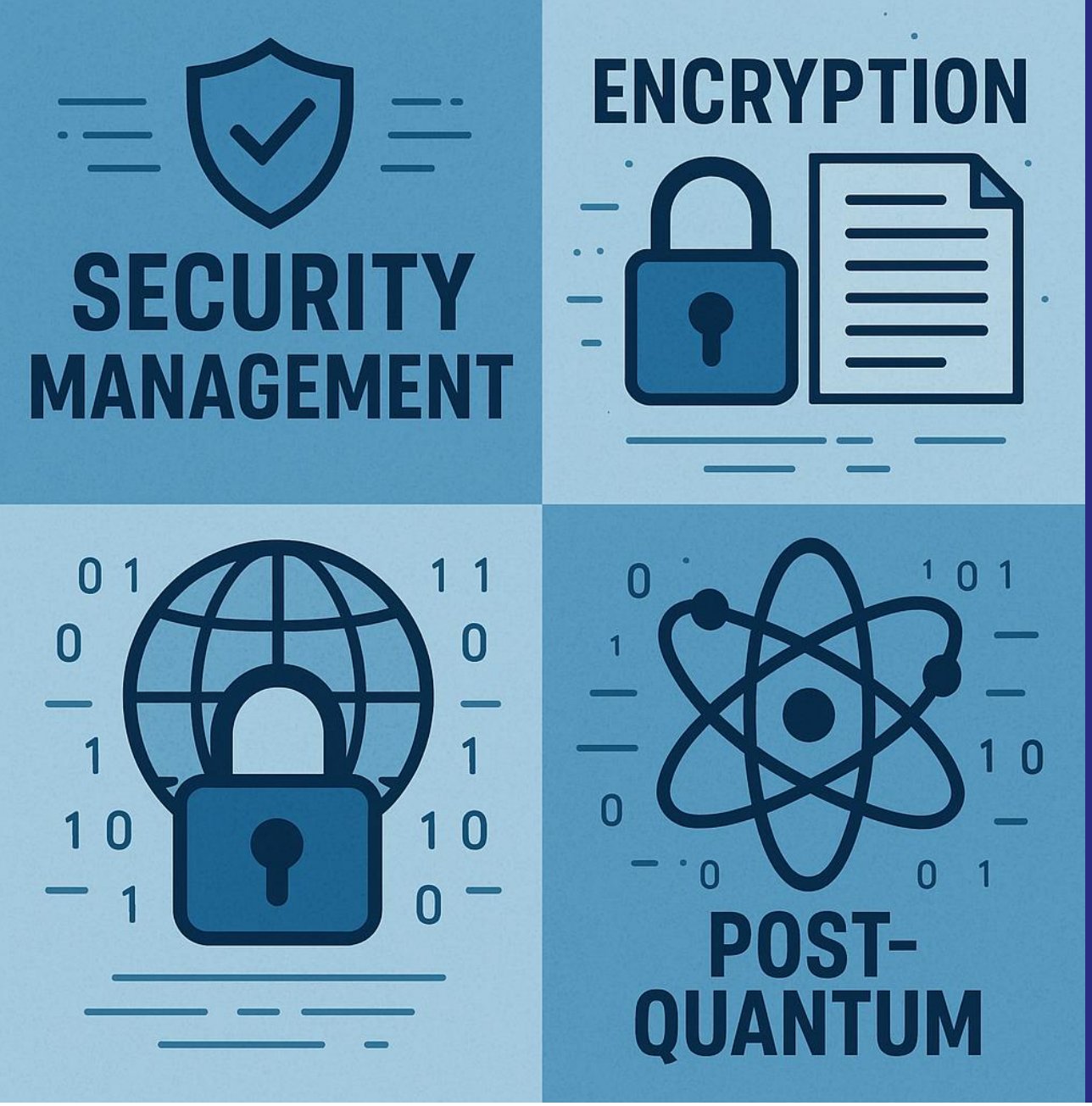
Preparing for migration is an opportunity

State of the art

Interoperability

No regret move

- Incidents handling
- Knowledge and vulnerability
- Operational agility



Preparing for the quantum threat should become an important aspect of security management

PQC : solutions

Solutions

- Symmetric Algorithms ➔ **Mild risk** (Grover's algorithm)

We can use longer keys and longer hashes (parameters)

- Asymmetric algorithms ➔ **Will be broken** by **Shor's algorithm**

Solution: new algorithms; new mathematical problems

Hybrid solutions

Combination: **Pre-quantum** algorithm + **Post-Quantum** algorithm

Example: *a hybrid signature*

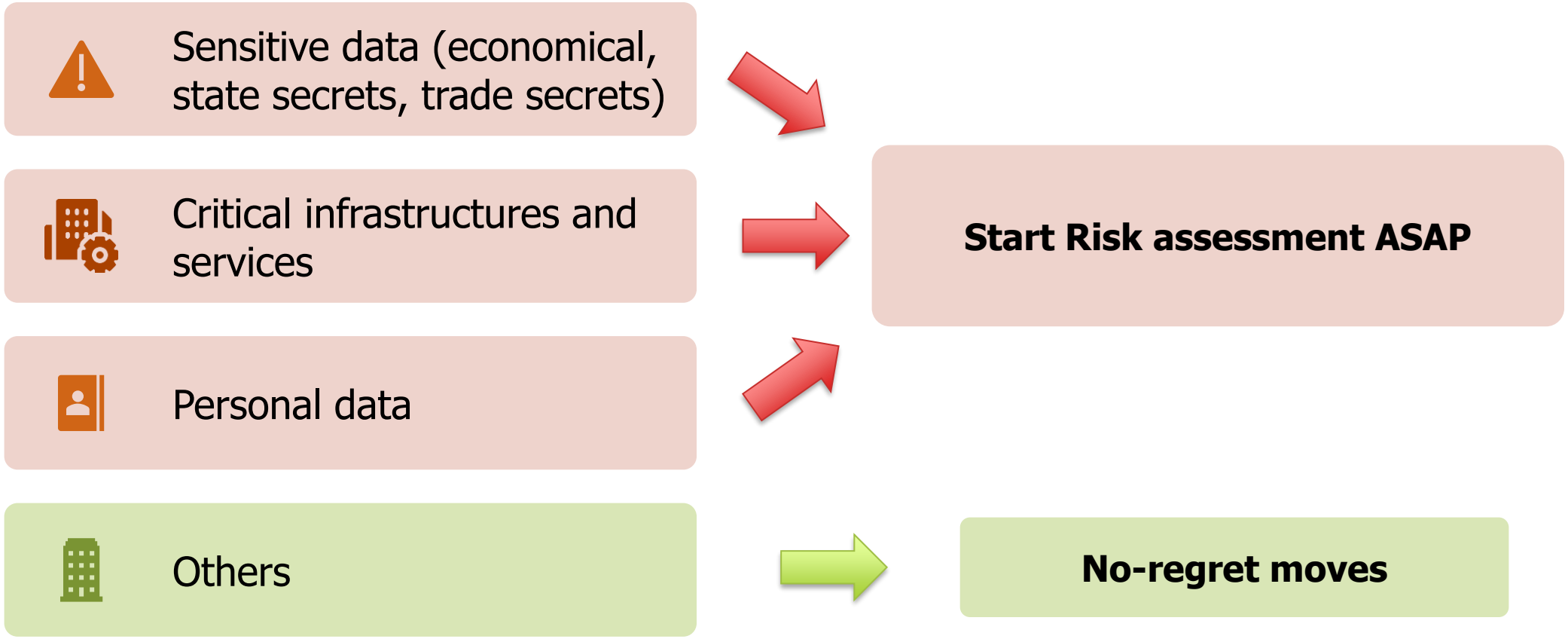
$$sign_{Hybrid}(message) = sign_{traditionnal}(message) \;||\; sign_{PQC}(message)$$

Hybrid solutions

Hybrid Solution	Only Post Quantum algorithm
Proven maturity of traditional cryptography	Simpler
More complex to implement	Riskier (still maturing)
More complex to operate	

Migration :
How to establish the roadmap

Type of companies



Roadmap – Planning

1. Assets & cryptography inventories
2. Risks assessment
3. Plan risk-oriented migration

4. Migration execution
5. Continuous research

Inventories

- Cryptographic assets inventory
- Vendors dependencies inventory
- Data assets inventory

Inventory of Cryptographic Assets

Goal:

- Exhaustive list of uses of cryptography

➔ Track all assets to migrate (algorithms, keys, certificates)

➔ Also handy outside of PQC migration

Most important part of the assessment

Update & Maintain & Protect

Inventory of Cryptographic Assets

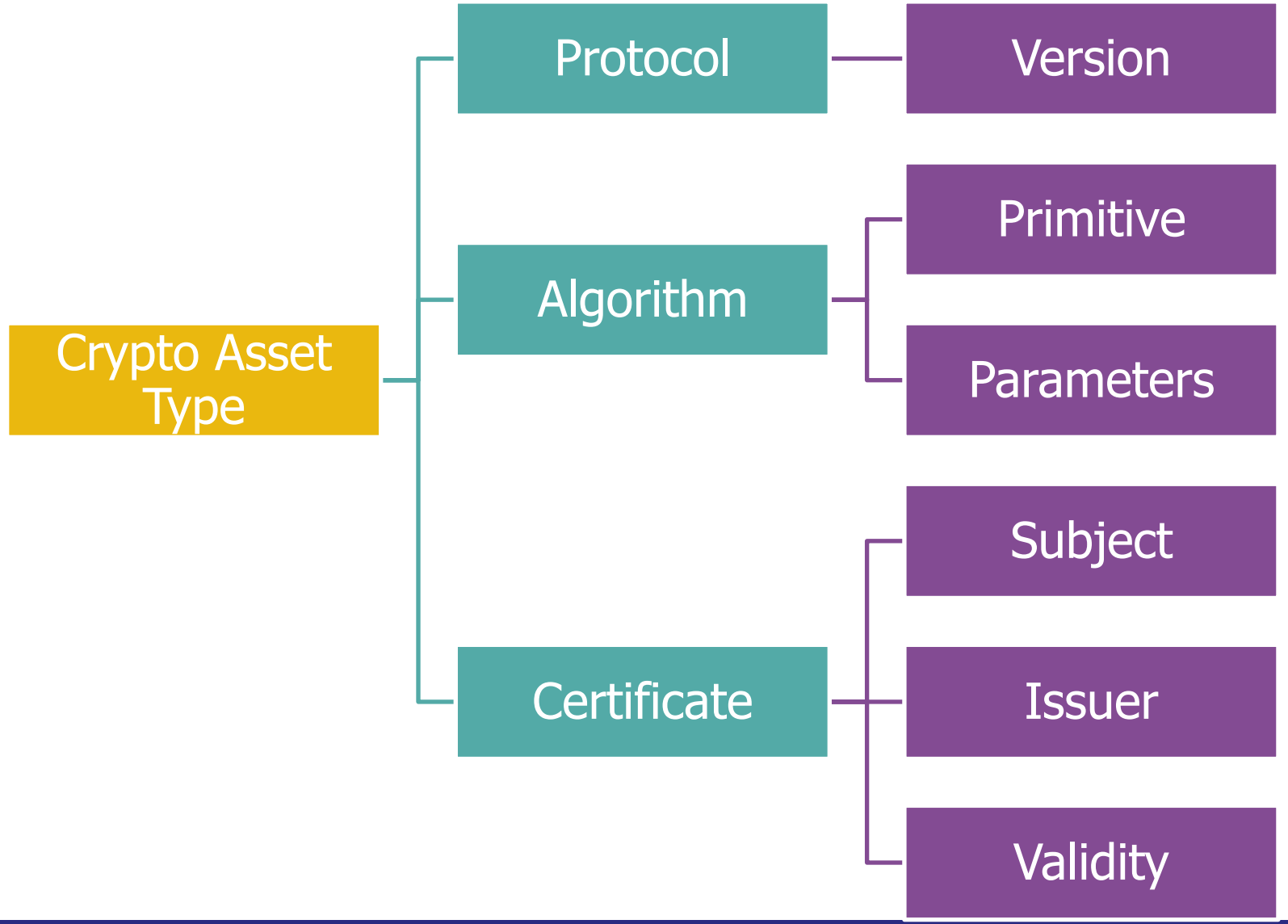
Standard formats

Ex: CBOM from IBM

➔Standard formats allow tools to generate part of the inventory

➔Some format allow dependencies reference

Inventory tools



Inventory of dependencies on vendors

Goal:

- Exhaustive list of cryptography depending on suppliers

- Products & services (Hardware, software, CA)
- (Planned) Support for PQC
- Contracts & contacts details

Shadow IT & additional tools (messaging, documentations)

Inventory of data assets

Goal:

- List of data handled by the organisation

- Type of data: data at rest, data in transit, data in use
- Location, Usages
- Value of the data
- Classification of data
- **Their protection**

Inventories

Risk assessment

- Cryptographic assets inventory
- Vendors dependencies inventory
- Data assets inventory

Risk assessment

➔ Prioritize assets to migrate

➔ Anticipate consequences

Risk

- Threat ➔ Attacker using Quantum Computers
- Vulnerability ➔ PQC vulnerabilities
- Impact ➔ What if ?

- **+ Time and effort to migrate**

Risk assessment: Lifetime of data assets

➔Identify **lifetime** of your information assets

- Business value
- Regulatory requirements
- Security reasons
- Confidentiality

➔ Lifetime & impact

Risk assessment: Infrastructure migration time

➔Estimate the time required to migrate technical infrastructure

- Current technologies
- Current procedures

- Available quantum-safe cryptography
- Discussion with suppliers

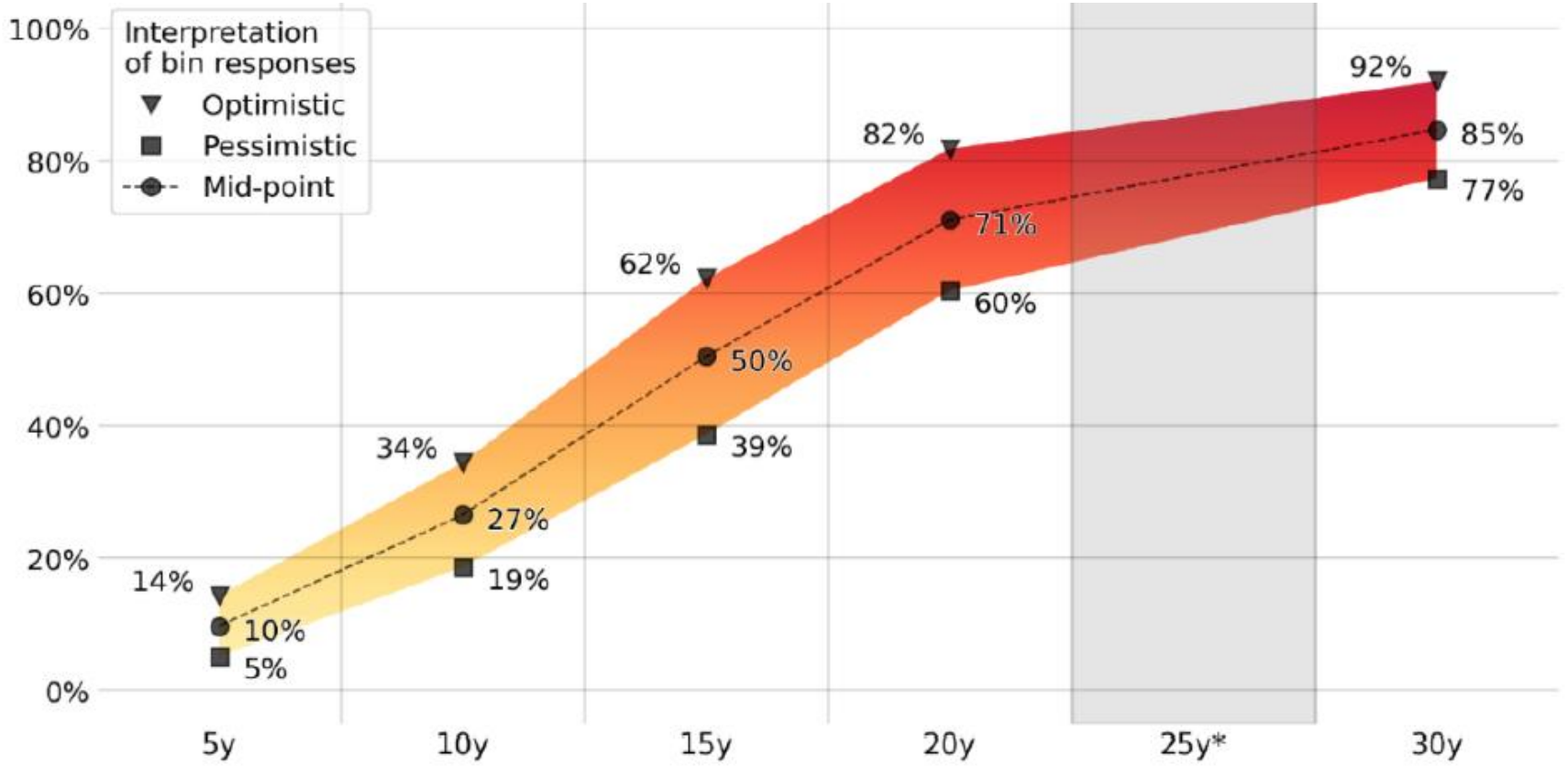
➔ Time information + migration steps information

Risk assessment: time for threat actors to access quantum technology

➔Estimate time for threat actors to access quantum technologies

- Analyze quantum threats
  - Papers / Independant researchers
  - Industry experts
  - Guidelines

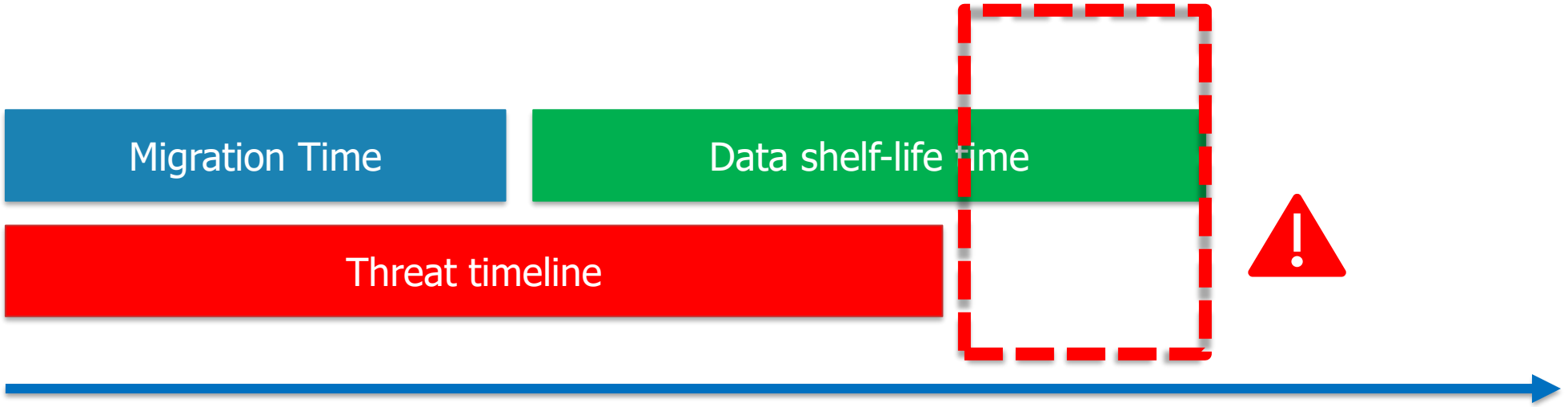
Assess the timing until current cyber defences collapse vs threat with access to quantum technology



[2024] 32 Experts estimates of likelihood of a quantum computer able to break RSA-2048 in 24hours

Risk assessment – Quantum Risk

➔Determine quantum risk by calculating whether assets will become vulnerable before the organization can move to protect them (Mosca's inequality)



If $T_{Migration} + T_{Shelf-Life} > T_{Threat}$ ➔ Risk

Migration planning

Goal

➔ For each cryptographic asset, **decide** if, when and how to migrate

➔ Decide priorities / order

- Planning of testing & implementation

Migration risks

- Forgotten assets, dependancies
- No hardware
- New crypto vulnerabilities
- Standards updates and changes
- …

➔ Mitigation plan in case of problems

Exécution

Continuous research

Relationship with suppliers

Migration execution

Regulators and autorities

The role of the authorities

Supervision

Support

Forums & awareness

The decisions we make today will shape the security of tomorrow

Sources

- Quantum Threat Timeline Report 2024 , Mosca M & Piani M., December 2024
- A Methodology for Quantum Risk Assessment, Dr. Michele Mosca & John Mulholland, 2017
- The PQC Migration Handbook, AIVD & CWI & TNO, December 2024

What are the PQC solutions ?

Post-Quantum Cryptography (PQC)	
Why ?	**Advent of Quantum Computers**
What ?	Key establishment + others
How ?	Transmission of **classical signals**
Why it works ?	**Mathematical difficulty** to break the Confidientiality & integrity
When ?	Started mid 70's

Quantum Key distribution (QKD)	
Why ?	**Advent of Quantum Computers**
What ?	Achieve key establishment
How ?	Transmission of **quantum signals**
Why it works ?	**Physical impossibility** to break the confidentiality
When ?	Started in 1984

Same **problem**, different **solutions**

PQC is an efficient and cost-effective solution while QKD is not mature yet

Discovery of Cryptographic Assets

Software development	Systems and applications	Network traffic	Hardware
• Cryptographic libraries • Custom crypto components	• VPN • IAM • Data encryption	• PKI • SSH, TLS, sFTP • IPSec	• HSM • Products
Tool / Process in the software dev Life Cycle	Asset Management	Network Analysis	Asset Management

Migration plan – Info for timing

- Crypto **agility** => Prepare to Quick updates
- Maintain operations ➔ **isolate** domains (PQC and preQC)
- Store now decrypt later attacks ➔ Sensitivity + protection period
- Prioritization: business & regulation priorities,
- Planning of **testing** & implementation
- Budgeting

=> Takes a lot of time