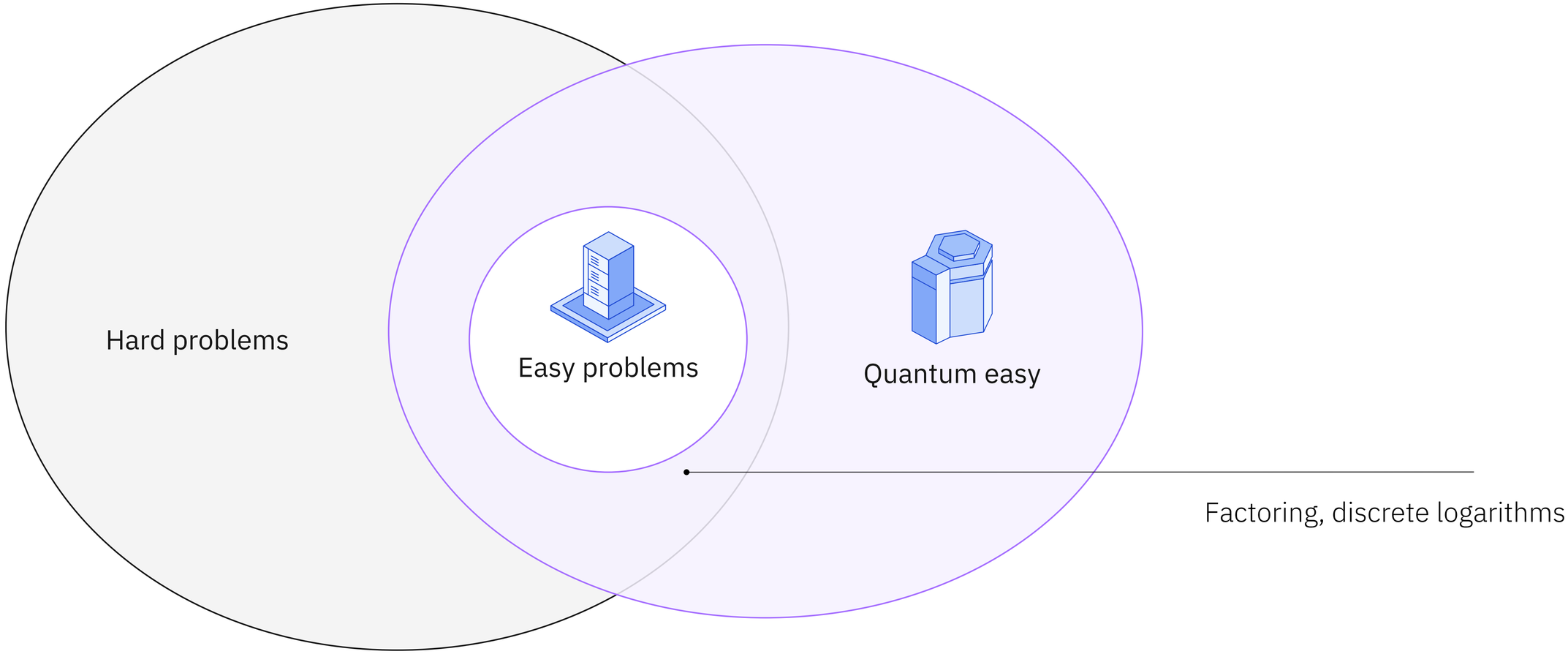
MINDSHARE
2025 10–11 SEP
CYBERSECURITY LEADERSHIP FORUM
Securing Identity for our Digital Future

Dr. Efstathia Katsigianni
IBM Research

Migrating to Quantum Safe

The source of quantum risk

There is a rich seam of problems that cannot be solved by classical and AI supercomputing, and never will. These are the trillion-dollar problems that quantum computing was designed to solve.



NIST standardization for Quantum-Safe Cryptography
NIST Standards

Asymmetric algorithms need to be replaced with “quantum-safe” ones

NIST published in August 2024 the **final Standards** for 3 out of the 4 quantum-safe algorithms selected – more standards are expected in the next years

A lot of ongoing work for bringing those into **libraries, protocols, products**

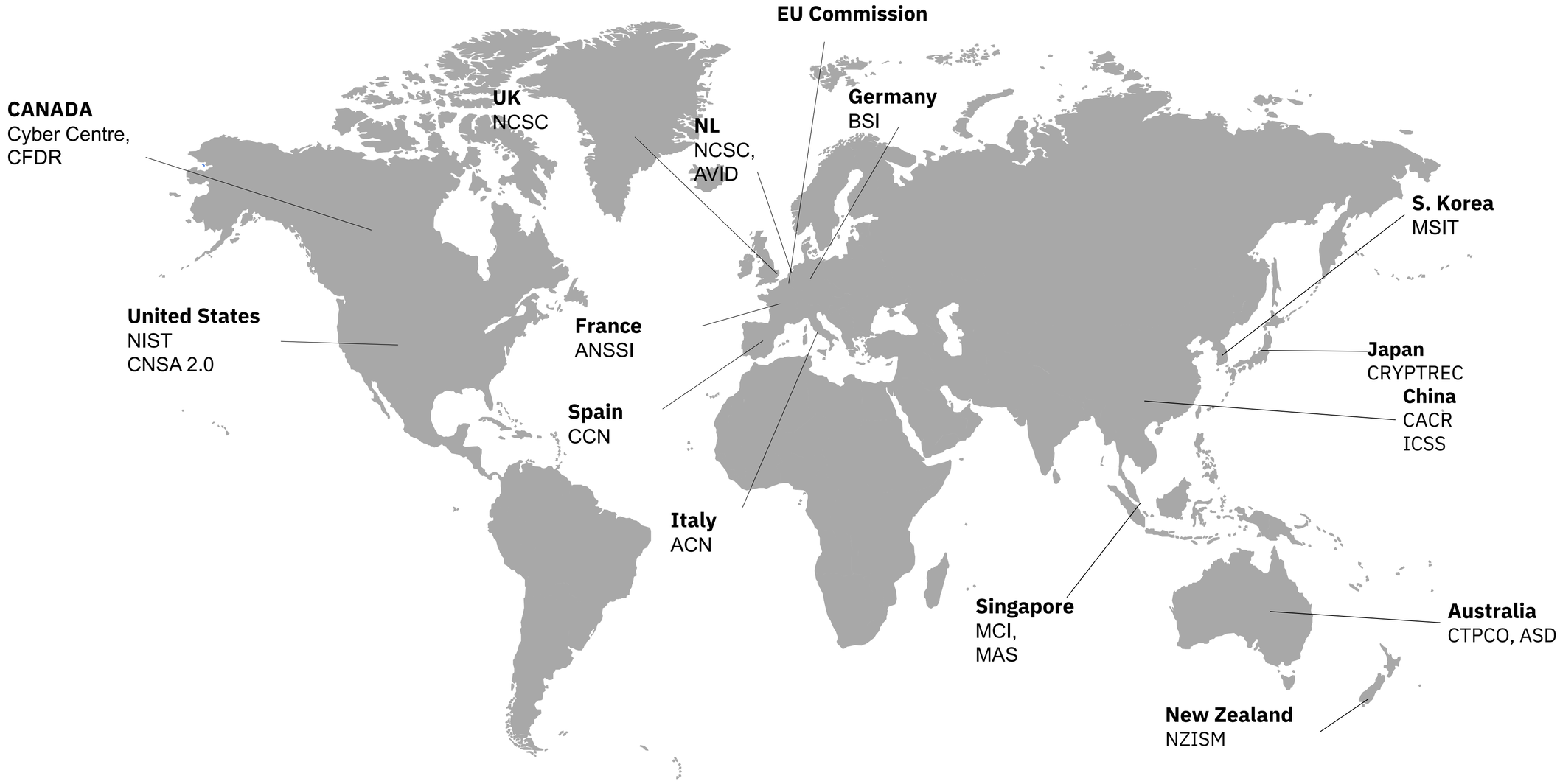
ML-KEM: Primary algorithm for Key encapsulation (to be used for key exchange)

ML-DSA: Primary algorithm for digital signatures

SLH-DSA: Stateless hash-based algorithm for digital signatures

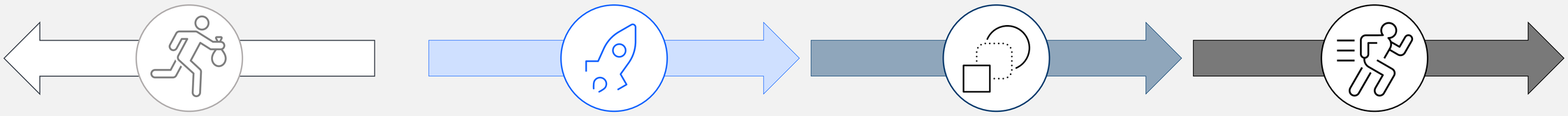
Globally, several recommendations for Post Quantum Cryptography are emerging

International recommendations converge to the early 2030s as a target for a complete migration



When will Cryptographically Relevant Quantum computers be available?

Rather than a single Q-Day, we expect Quantum Computers to gradually improve, therefore reducing the cost of a Quantum Attack



Before the availability of Quantum Computers - No Quantum attacks possible, but secrets are harvested

Capability Level 1
Moonshot
“cryptographically relevant” Quantum Computer

Few and expensive Quantum Attacks

Capability Level 2
Slow “cryptographically relevant” Quantum Computer at scale

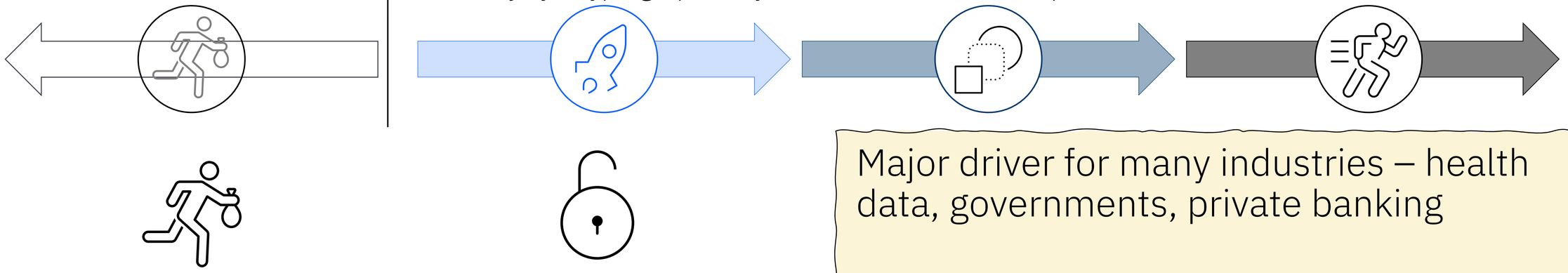
Low-cost Quantum Attacks

Capability Level 3
Fast “cryptographically relevant” Quantum Computer

Active Quantum Attacks

Primary threats and drivers

Availability of "cryptographically relevant" Quantum Computer



Harvest confidential data
in order to decrypt them later

Decrypt lost or harvested confidential data through stealing encryption keys

Major driver for many industries – health data, governments, private banking

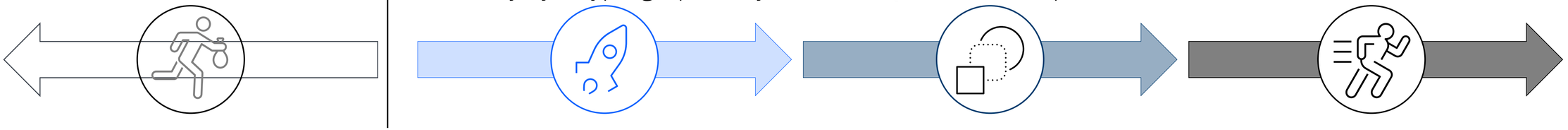
Data security regulations are a major factor

Requires targeted actions for risk mitigation

Requires prioritization; which are the data that are highly sensitive & exposed?

Primary threats and drivers

Availability of "cryptographically relevant" Quantum Computer

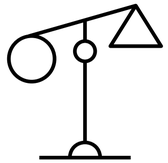


Manipulation of legal history a major driver for some industries, such as government, banking

Complex multi-year project, whole business ecosystem affected

Needed: establish foundation for efficient/controlled/risk-based execution, in line with current ways of working

Manipulate firmware updates & transactions through fraudulent **authentication**



Manipulate digitally signed contracts & legal history by **forging digital signatures**

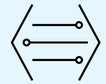
Cryptography
The enterprise context

Governance

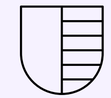
Data

Applications

Development

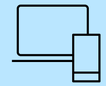


Security



Infrastructure

Devices



Cryptographic modules

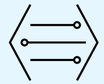
Cryptography
The enterprise context

Governance
Policies and procedures
National or Sector Guidelines
Standards
Certification
Compliance
Processes

Data
PII
Databases, Data Lakes
Signed documents

Applications
APIs
API Gateways
Service providers
Third-party components
Applications
Legacy Applications
Third Party Applications
Source code
Open/closed source libraries

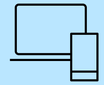
Development
Tools
CI/CD
Automation
Configuration
Testing & QA



Security
PKI/CA and Certificates
Security Management (SIEM and SOAR)
Identity & Access Management
Privilege Access Management
Key Management
Protocols: TLS, HTTPS etc.
Cryptographic APIs (PKCS11)

Infrastructure
Infrastructure/Boot stack
Cloud platforms
Networks
Storage

Devices
Devices/IoT
Cards

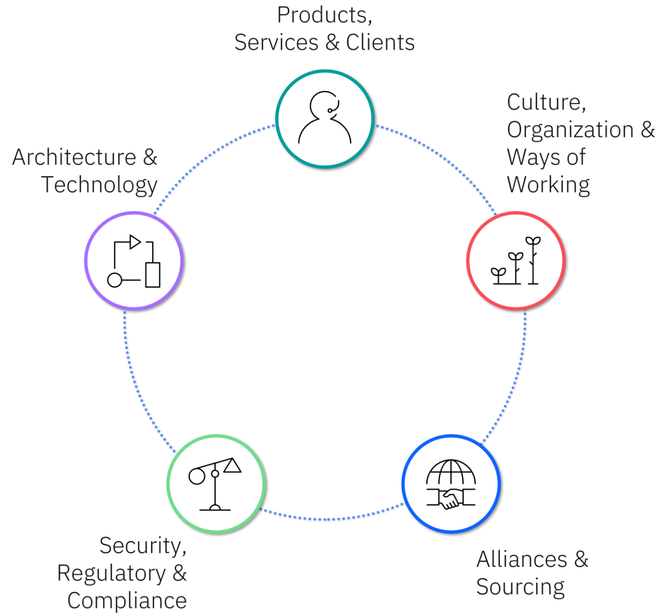


Cryptographic modules
Enclaves
HSMs
Entropy
Tokens

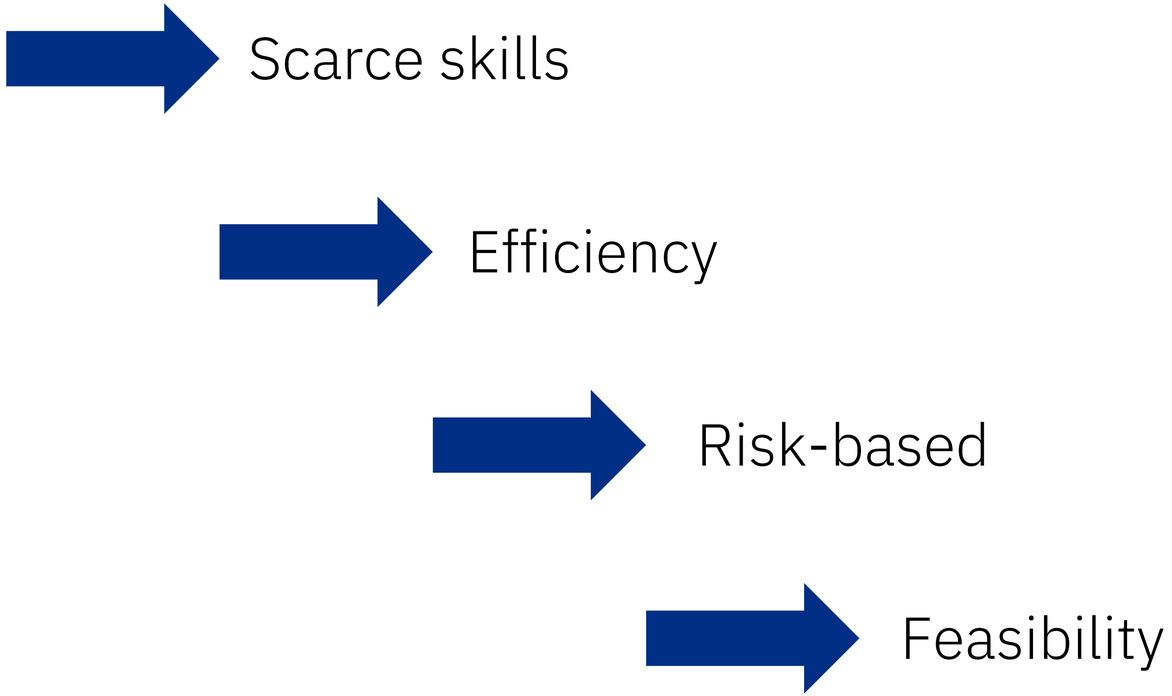
Transformation key constraints

A typical organization faces many challenges from the beginning of their Quantum Safe transformation:

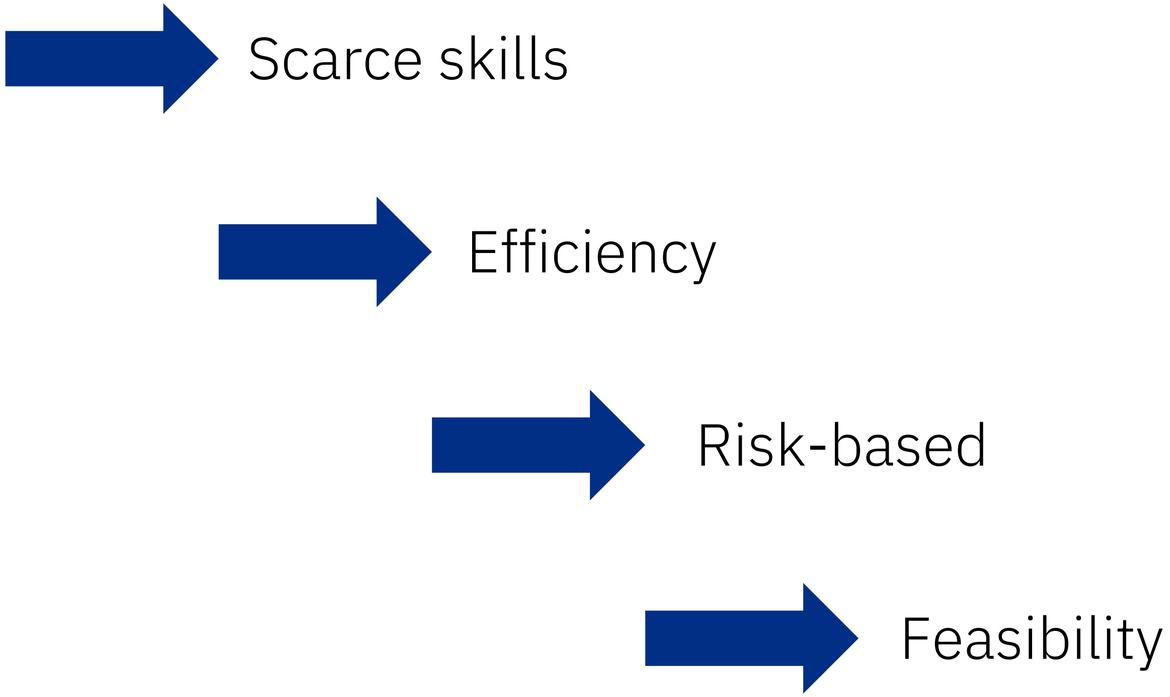
- Obtaining management buy-in & getting mandate to act
- Identifying the right stakeholders
- Prioritizing quantum-safe activities within daily job
- Prioritizing quantum-safe wrt other cybersecurity threats
- Being able to “absorb” the extent of necessary activities
- “Distractions”



Transformation key constraints



Transformation key constraints



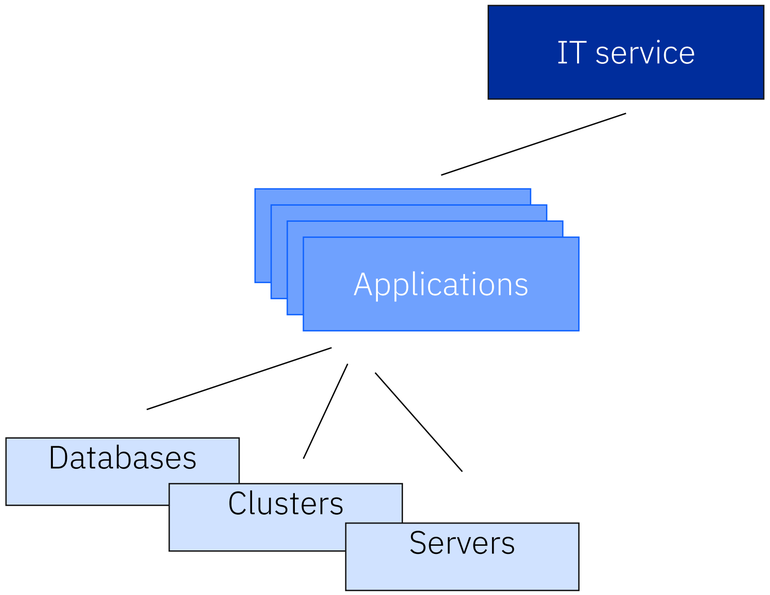
Build a central team to drive the quantum-safe transformation

Re-use insights from regulators & industry

Incorporate activities in overall cryptographic governance

Apply pre-defined and validated patterns where feasible

Focus on a high-level cryptographic inventory as the first step



Initial focus was set by many on a detailed cryptographic inventory for operations and source-code, but:

- Using the collected insights is hard without context
- Many false positives, very high initial effort with limited gains

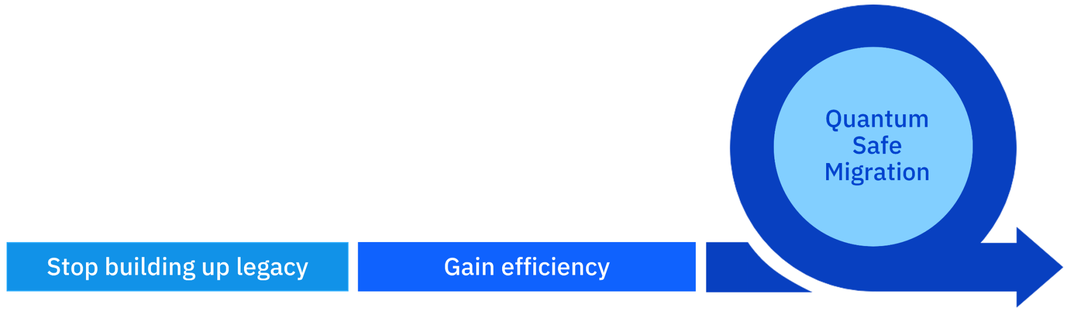
Prioritization should be driven by business criticality of an asset – can be done on IT-Service level

Focusing on **external** critical flows, it is possible to define urgent actions

Identify **dependencies** in more and more depth to drive the migration planning

Create an agile transformation plan

- Transformation plan needs to be **constantly adjusted** according to risk, re-prioritization, and feasibility of actions
- A clear management **mandate** is needed
- Early focused preparation & actions in “fundamental cryptographic services” – e.g., **PKIs**, as well as **procurement**, **cryptographic governance** are key
- Focusing on network perimeter & common infrastructure
- Individual teams need **central guidance** – which algorithms to choose, which technical dependencies to consider, what is the direction of protocol standardization, what to ask from suppliers, etc



Client case study
Client Journey: European Banking Group (incl. Insurance Business)

Client Profile & Challenge

- Technology provider for large Banking Group with entities across Europe
- Awareness of quantum threat, but no view on QS priorities
- Cryptographic governance not well defined or documented

Payment-specific infrastructure is a high priority use-cases

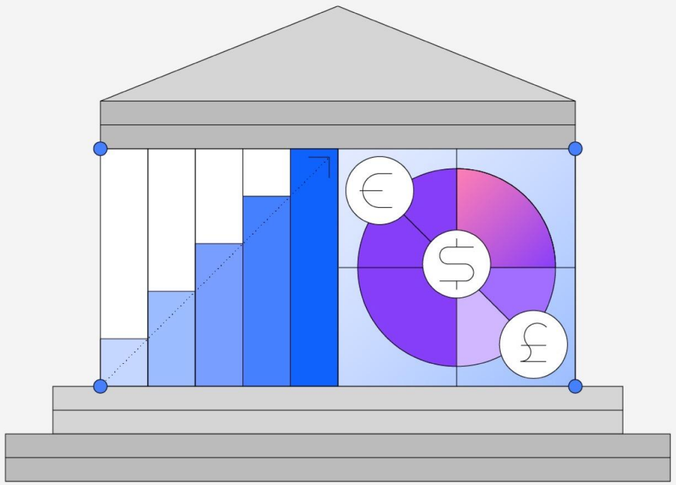
--some parts are depending on payment-specific regulations

Complex PKI landscape – “to hybrid or not to hybrid?”

Internally-developed cryptographic services in need of adaption

Governance of the quantum-safe program within the organization clashes with the internal structure

➔ Complex multi-year transformation



Client case study
A large international telco operating in many countries.

Client Profile & Challenge

- Large, multi-national telco
- 20+ operating countries
- Diverse vendor landscape
- Struggling with cryptographic posture management
- Unaware of order of magnitude of problem across product, organizational, and infrastructure landscapes

Observability/monitoring is challenging on telco components

What does **cryptographic agility** mean?

→ Major focus on updateability of products in the field.. Translating into:

- Requirements for suppliers
- Requirements for internal development
- Requirements and adaptations to internal processes

Changes depending on telco-specific standards

IoT-devices in scope pose strict requirements

➔ Complex multi-year transformation with group <-> local markets coordination

Key take-aways

Quantum threatens our digital security

Quantum computers **threaten current cryptography**

The Quantum Threat is already **relevant today**

But cryptography is **difficult to replace**

Industry sectors and Governments recommend to act

New cryptographic algorithms have been developed and standardized

Leading nations have **incorporated quantum-safe** preparation into their national quantum strategies

Entities such as the European Commission encourages Member States to develop a **comprehensive strategy** for the adoption of Post-Quantum Cryptography

Organizations should take a re-usable approach

Organizations must **prioritize** their efforts to address the quantum threat

A **risk framework** should be used to identify and prioritize areas of high risk

A **central team** approach is required to manage the complexity

MINDSHARE
2025 10–11 SEP
CYBERSECURITY LEADERSHIP FORUM
Securing Identity for our Digital Future

IBM

Questions

Dr. Efstathia Katsigianni
IBM Research