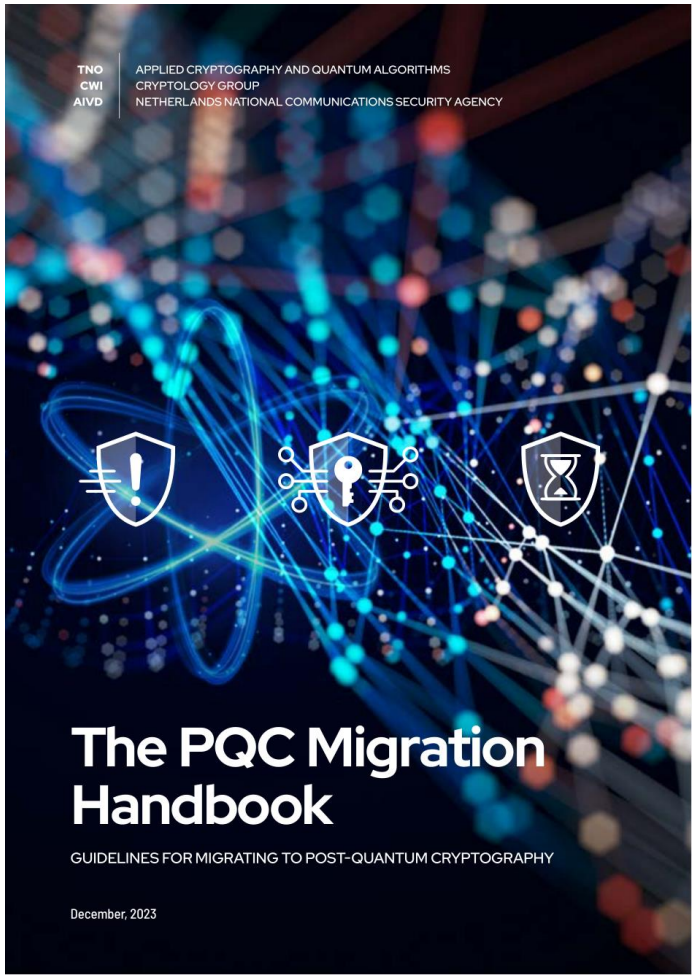
The PQC Migration Handbook
Revised and Extended 2nd Edition

&

Cryptographic Asset Discovery

Marc Stevens (CWI),
Anita Wehmann (MinBZK) & Maaike van Leuken (TNO)

The PQC Migration Handbook



- 1st PQC Migration Handbook published in March 2023
- Collaboration between AIVD, CWI & TNO

- Handbook Goal: pave the way for PQC migration in practice
  - Concrete, current and hands-on advice and action steps

- Collection of state-of-the-art advice from NIST, ETSI, IETF, etc.
  - Corporate insights from FoxCrypto, NXP, Deloitte, KPMG, KPN, …
  - Governmental insights from (Dutch) Ministeries

Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

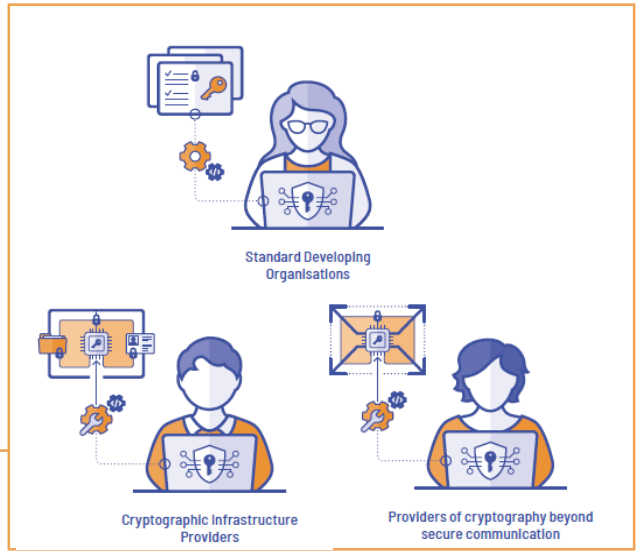
CWI

TNO

The PQC Migration Handbook

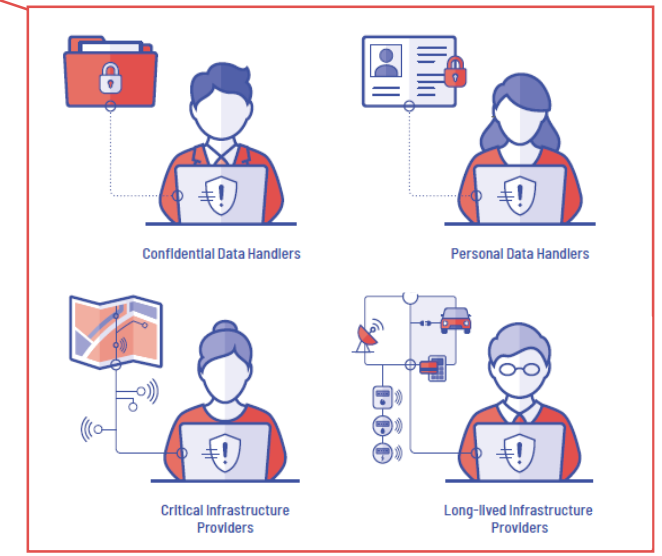
Three-step approach by ETSI

- Step 1: Diagnosis
  - **PQC Personas**
  - **PQC Inventory**

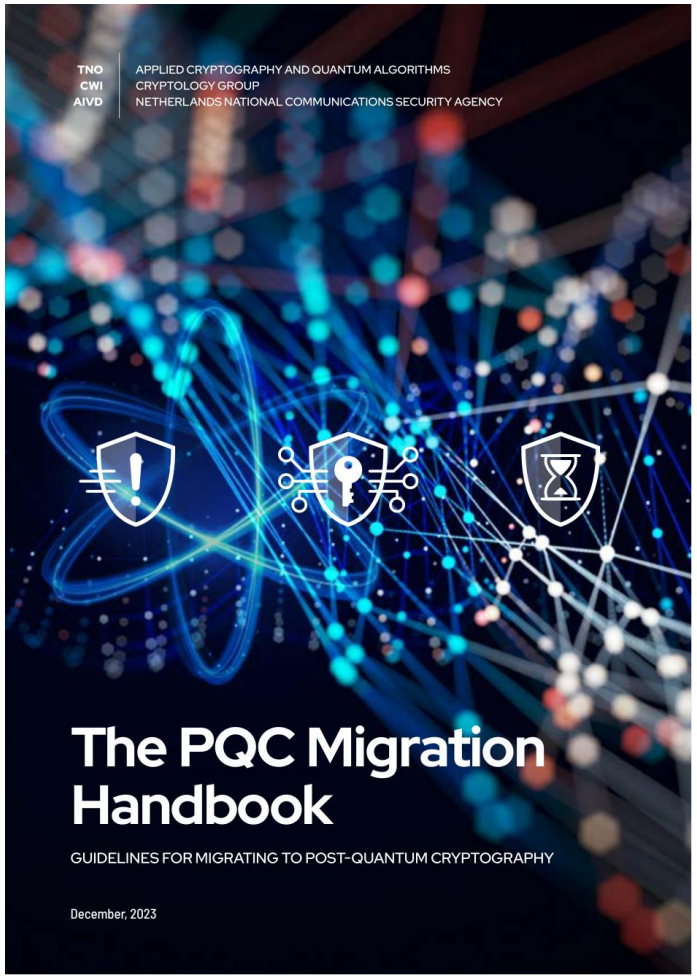


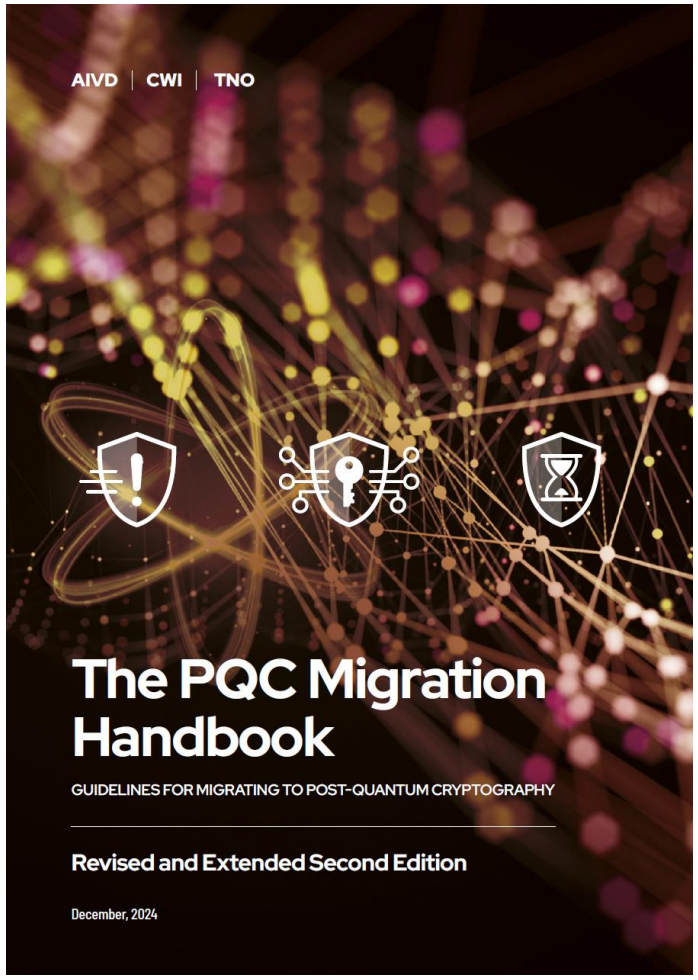
- Step 2: Planning
  - When?: Using **Migration Scenarios**: $X + Y_i + W_i < Z$
  - How?:
    Business Planning: Manager, Team, Budget, other organizations
    Technical Planning: Asset Migration Dependency & Order, Testing

- Step 3: Execution
  - Choose migration per cryptographic asset: **Replace/Redesign/Retire**
  - General strategies such as **Hybrid** & **Pre-Shared Keys**
  - **Cryptographic Agility**



The PQC Migration Handbook
Revised and Extended 2nd Edition





- New project between AIVD, CWI & TNO
  - April – December
- 1st Edition Limitations
  - New PQC Standards unfinished
  - Aimed at preparing organizations
- 2nd Edition Goals
  - **Incorporate feedback** on 1st Edition
  - **Revise** based on recent developments
  - **Extend** in many areas
- Content almost doubled from 62 pages to 117 pages.

Thanks to our team & community

PQC Handbook 2nd Edition Team

- Alessandro Amadori (TNO)
- Thomas Attema (CWI & TNO)
- Maxime Bombar (CWI)
- Ronald Cramer (CWI & U. Leiden)
- Vincent Dunning (TNO)
- Simona Etinski (CWI)
- Daniël van Gent (CWI)
- Marc Stevens (CWI)
- AIVD Cryptologists & Advisors

Acknowledgements

- The many people from

  ABN Amro, Auditdienst Rijk, Cloudflare, Deloitte, DICTU, Dutch Banking Association, Ericsson, Fox Crypto, Keysight Technologies, King's College London, KPMG, KPN, Max Planck Institute for Security and Privacy, Min BZK, Min I&W, Min OCW, Min VWS, NCSC-NL, NXP Semiconductors, Radboud University, TU Delft, TU Eindhoven, Quantum Gateway Foundation

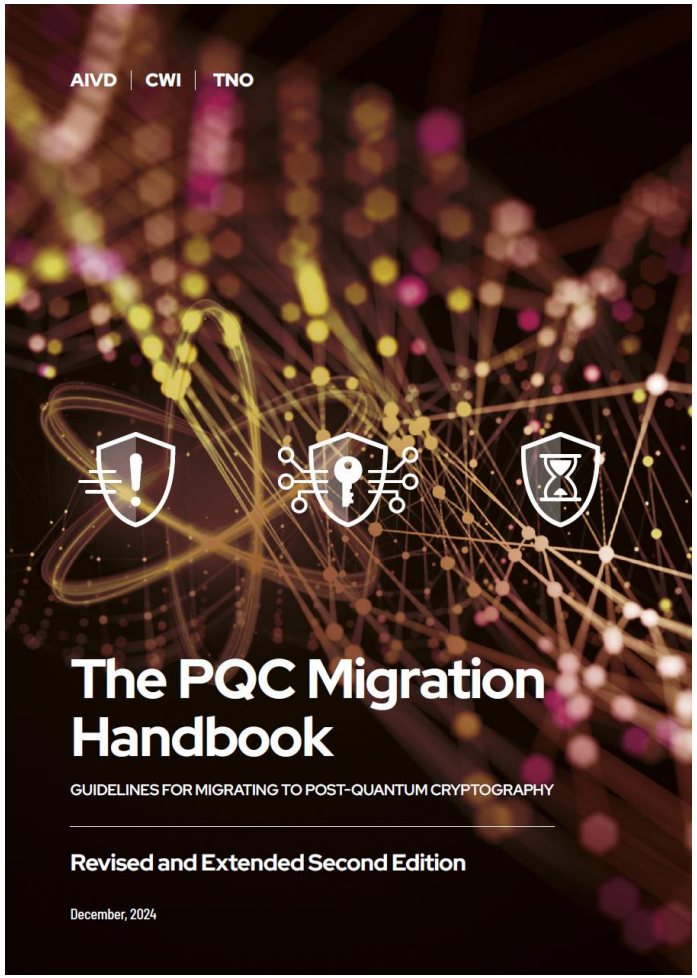
  for their feedback & contributions.

Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

CWI

TNO

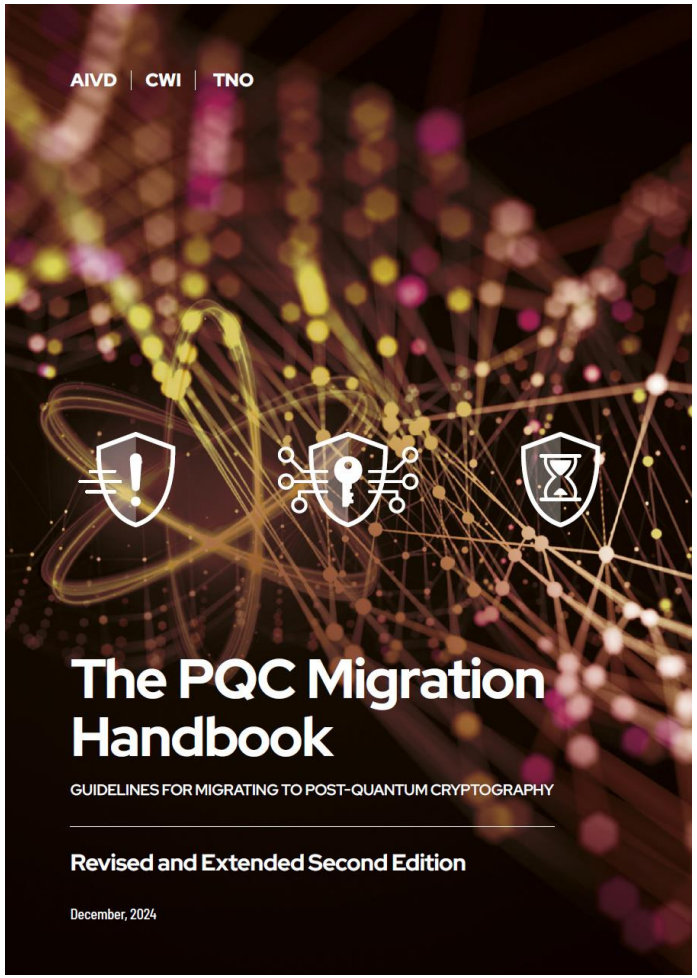
The PQC Migration Handbook
Revised and Extended 2nd Edition



Highlights new material:

- No-Regret Moves (Ch.1.6)
- Cryptographic Asset Management (Ch.2.3)
- Cryptographic Agility (Ch.4.4)
- Quantum Risk Assessment (Ch.2.4)
- PQC Migration Maturity Assessment (Ch.3.2.2)
- Overview International Developments (Ch.5)
  - Relevant Standardization & Legislation
  - Other published PQC Guidelines & Advice
  - Lessons learnt from Executed PQC Migrations

The PQC Migration Handbook
Revised and Extended 2nd Edition



- No-Regret Moves
- Overview International Developments
  - Relevant Standardization & Legislation
  - Other published PQC Guidelines & Advice
  - Lessons learnt from Executed PQC Migrations
- Research Project on Cryptographic Asset Discovery
  - Contributed section to 2nd Edition PQC Migration Handbook

The PQC Migration Handbook
No-Regret Moves – Section 1.6

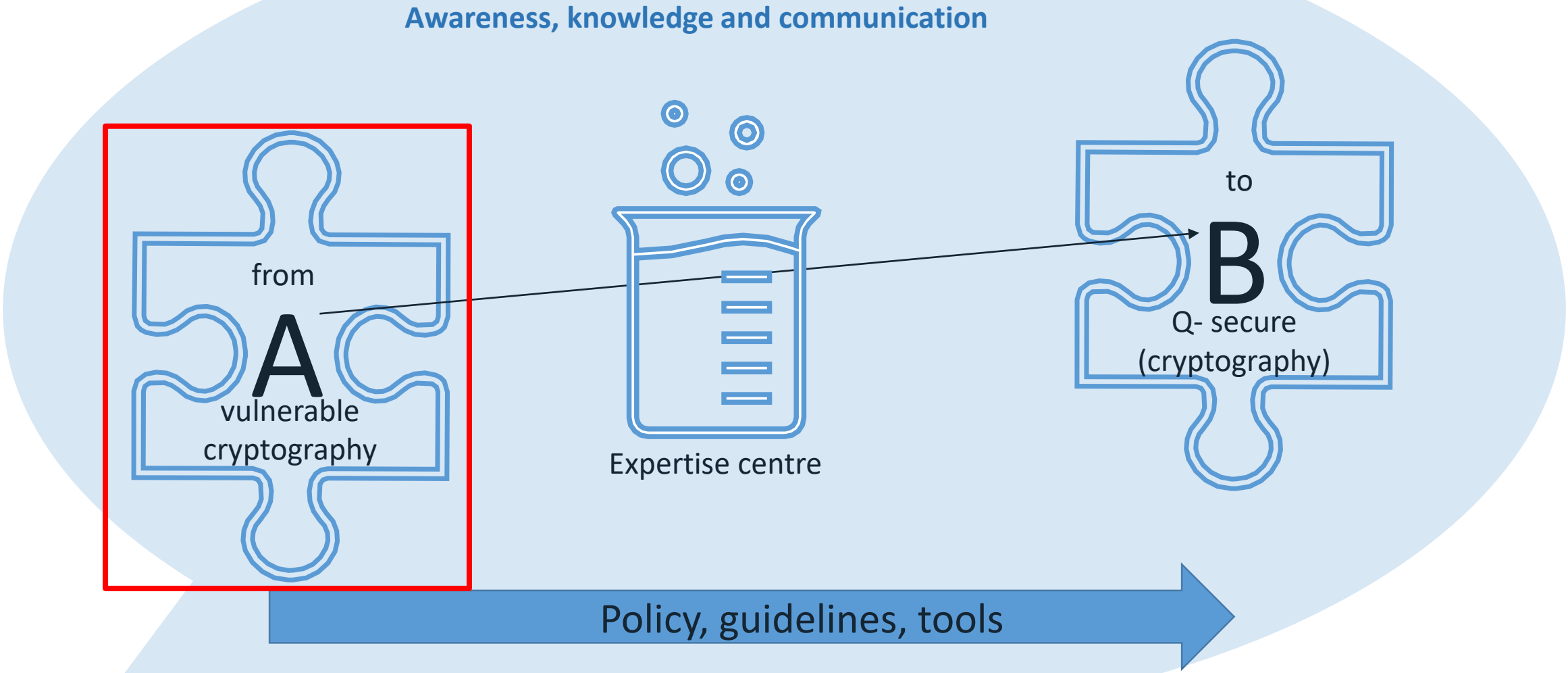
- Establish Cryptographic Asset Management (detailed in Ch.1.7 & 2.3)
- Review Cryptographic Policies (Ch.2.3 & 4.4)
- Conduct Risk Assessment (Ch.2.4)
- Estimate Costs of Migration (Ch.3.3)
- Inventory Regulatory Requirements (Ch.5)
- Provide a Back-Up Plan for quantum computing or cryptanalytic breakthrough
- Assess Supply Chain Dependencies (Ch.2.1)
- Collaborate with Peers

The PQC Migration Handbook
New Chapter 5 – Recent Developments

- Standardization Initiatives
  - NIST (Competitions, SHB), ISO (SHB, ML-KEM + McEliece, Frodo)
  - IETF (WG: PQUIP, TLS, ACME, …), ETSI (migration advice, follows NIST), …
- PQC & Legislation
  - Security: US (FIPS, FISMA), EU (NIS2, GDPR), ISO/IEC (27000)
  - PQC: US (WH-Memorandum, CNSA)
- Guidelines & Advice: EC Recommendations (11/4/24), Germany, France, Netherlands, UK
- Lessons learnt from Executed PQC Migrations
  - Google ALTS (Application Layer Transport Security): very high control & agility, session issues
  - PQ-TLS: Google+Cloudflare, Meta: hybrid with ML-KEM (drafts), network packet issues
  - PQ-Messaging: Signal, iMessage: incorporate hybrid KEM, ML-KEM, now formal verification

Cryptographic Asset Discovery

Transition to QsC simple model



Research: crypto inventory tooling

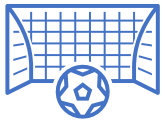
Initiative: program Quantum Secure (Safe) Cryptography Gov

Commissioning parties:

Ministry of the Interior and Kingdom Relations

National Cyber Security Centre (NCSC)

Ministry of Economic Affairs



Ambition: (first step to)

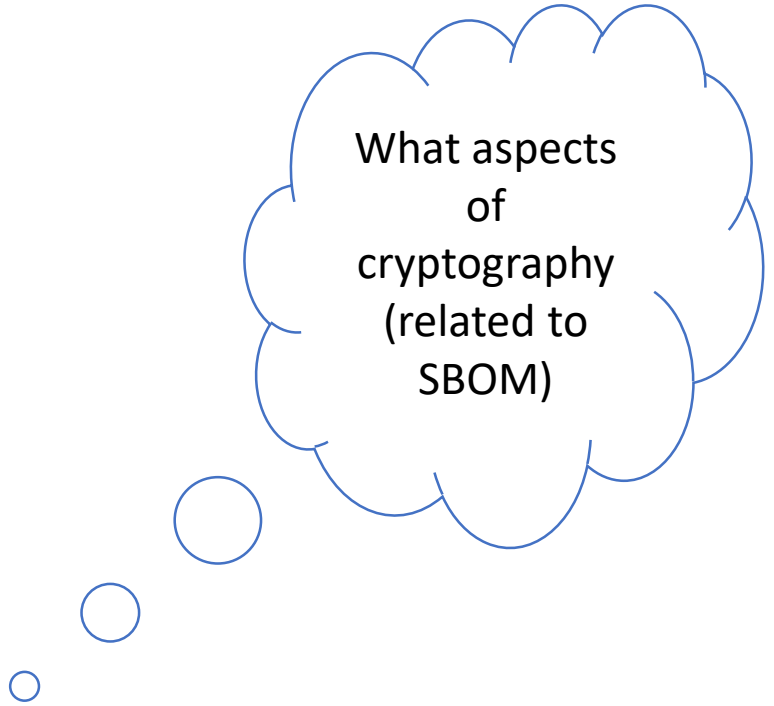
automated cryptographic assetmanagement

being part of IT (OT, IoT) assetmanagement

High level plan for the research

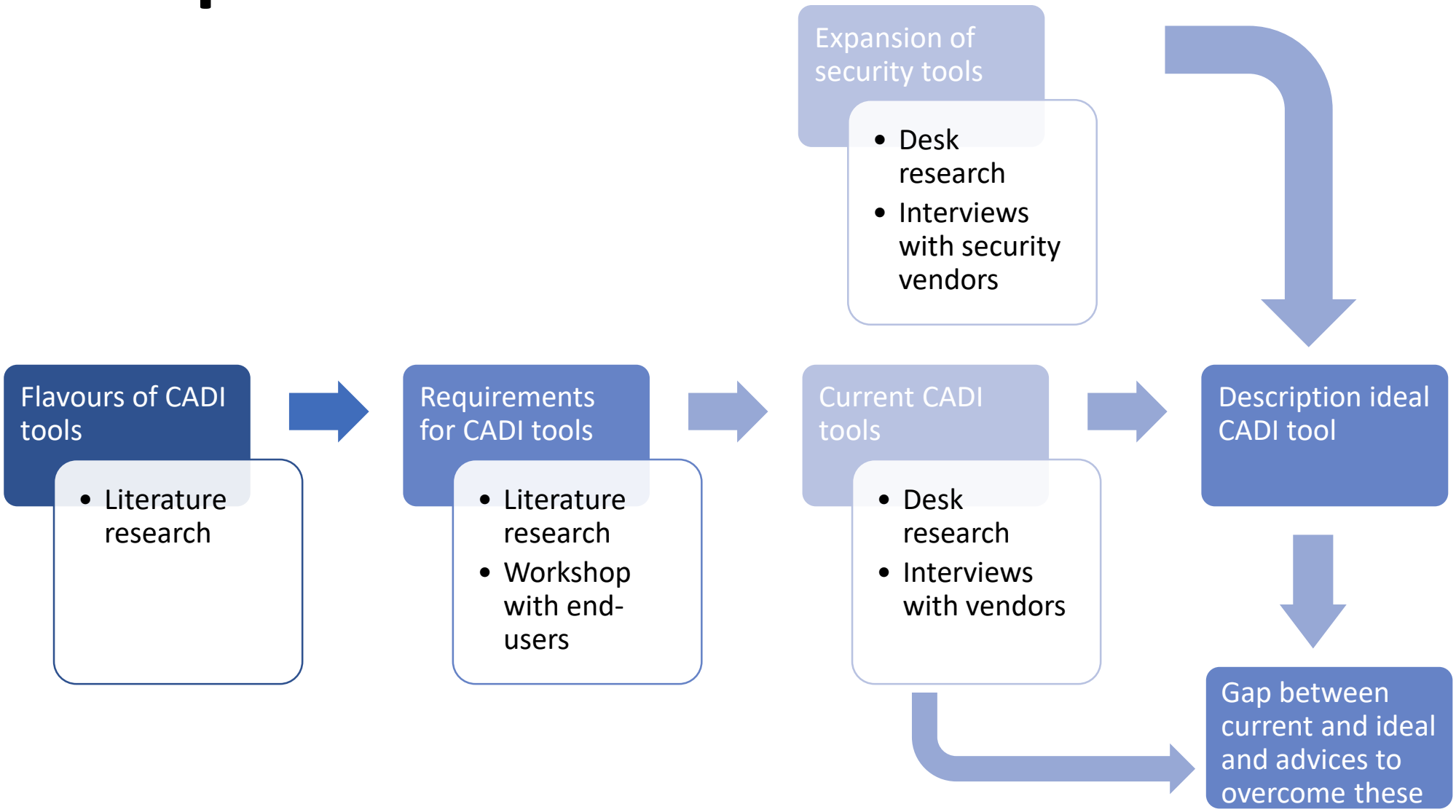
Investigate the fit gap between current capabilities of crypto inventory tooling and the MVP

Give advice how to overcome this fit gap



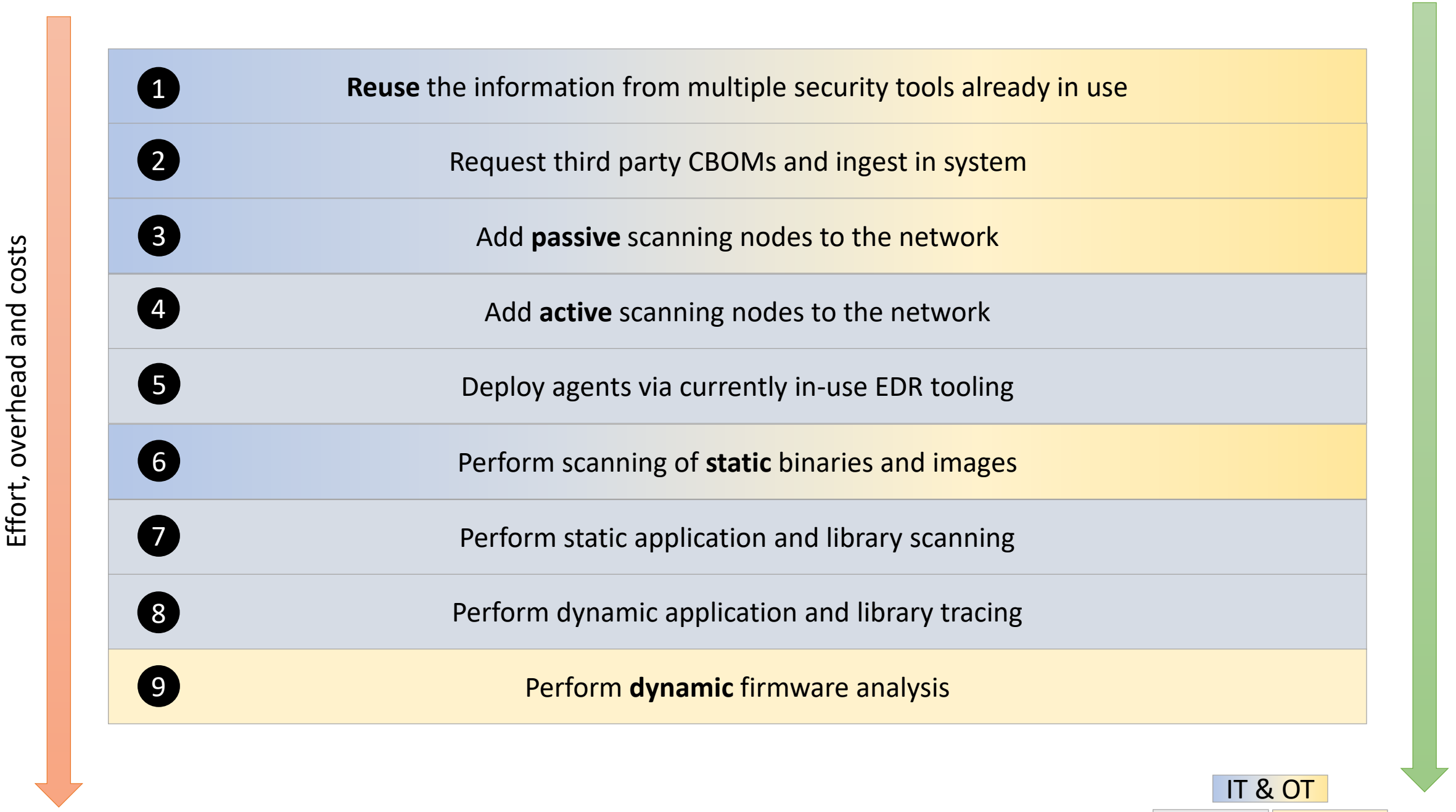
From a dream to a research approach

Set-up Research



Use case dependency

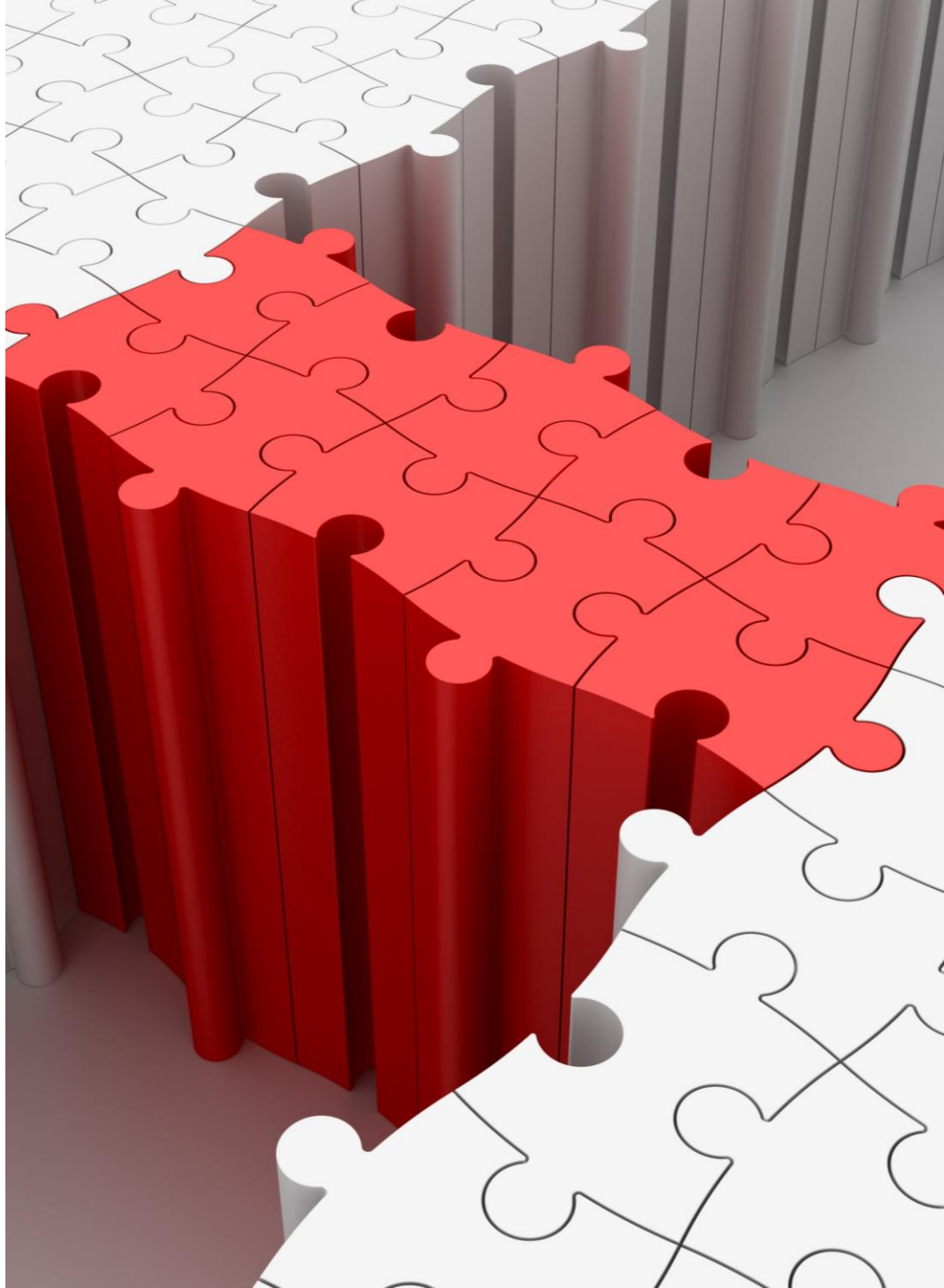
- Especially the distinction between IT and OT environments
- Balance between effort, overhead & costs versus accuracy & completeness


Effort, overhead and costs
1 Reuse the information from multiple security tools already in use
2 Request third party CBOMs and ingest in system
3 Add passive scanning nodes to the network
4 Add active scanning nodes to the network
5 Deploy agents via currently in-use EDR tooling
6 Perform scanning of static binaries and images
7 Perform static application and library scanning
8 Perform dynamic application and library tracing
9 Perform dynamic firmware analysis
Accuracy and completeness
IT & OT
IT
OT

Flavours of CADI tooling

		CADI			Security			
		A	B	C	I	II	III	IV
Network	Passive	X	X	X		X		
	Active	X	X	X	X	X		
Application and libraries	Static	X			X	X	X	
	Dynamic	X						
Firmware	Static				X			X
	Dynamic							
File system	Static	X	X					

Gaps		Advice
OT environments	→	Improving OT security
Validation	→	Set-up experiment



Wrap-up

- CADI is a no-regret move
- Any organisation should start with re-using information from security tools and request CBOMs from vendors
- Section on cryptographic asset management in the PQC Migration Handbook
- Thank you for your attention!