Post-Quantum

Cryptography Conference

Comparing Strategies for Quantum-Safe Cryptography Adoption in Organizations

Jaime Gómez García

Head of Quantum at Banco Santander

Santander

Block›chain

Comparing Strategies for Quantum-Safe Cryptography Adoption in Organizations

PQC Conference – PKI Consortium

Nov. 7th 2023

Jaime Gómez García (jaime.gomez@gruposantander.com)

jaime-gomez-garcia

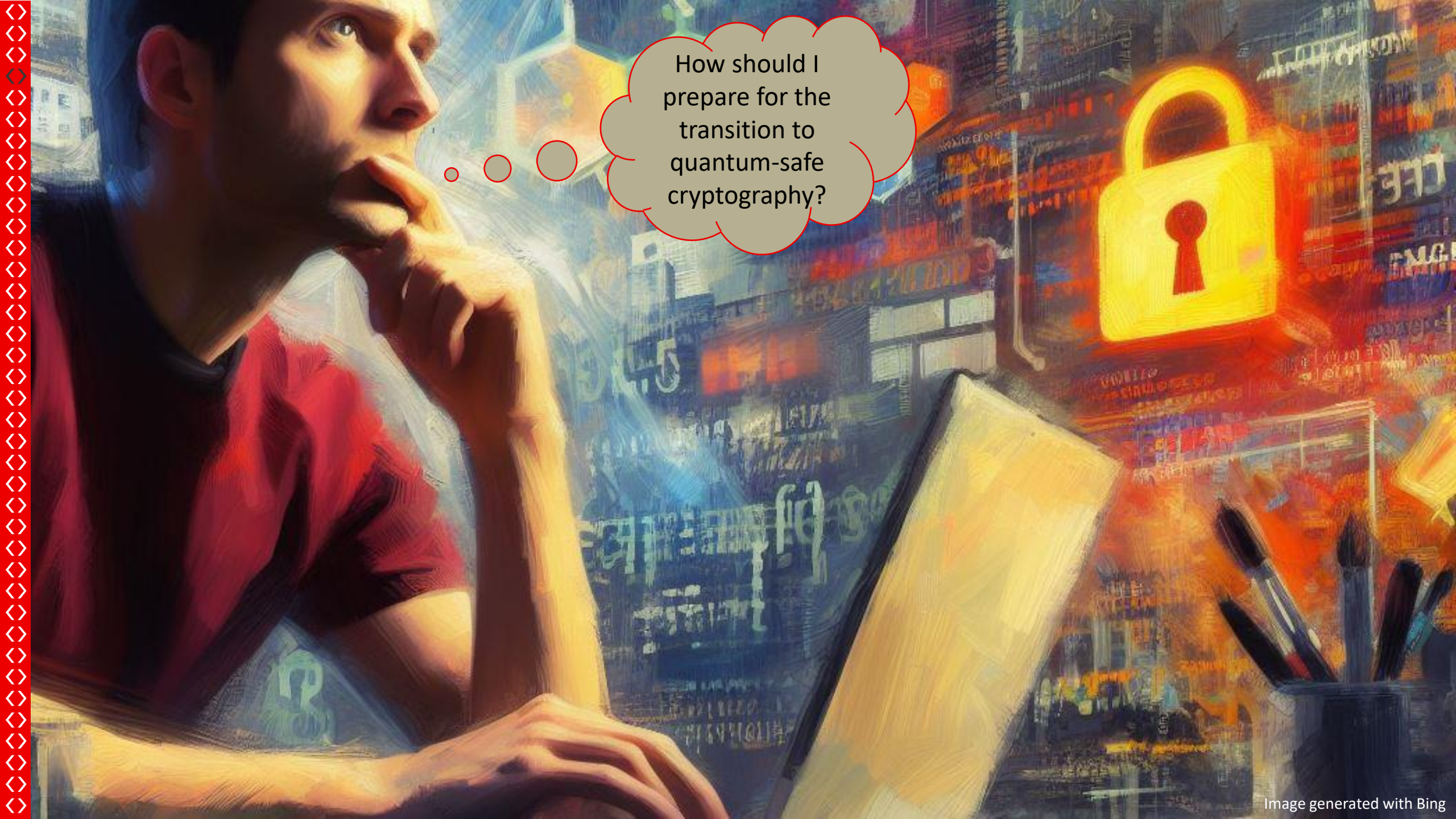


Image generated with Bing

An official website of the United States government Here's how you know

NIST

Search CSRC

CSRC MENU

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

PROJECTS

Post-Quantum Cryptography PQC

Overview

Draft FIPS 203, FIPS 204 and FIPS 205, which specify algorithms derived from CRYSTALS-Dilithium, CRYSTALS-Kyber and SPHINCS+, were published August 24, 2023. The public comment period will close November 22, 2023.

PQC Seminars
Next Talk: November 7, 2023

Additional Digital Signature Schemes - Round 1 Submissions

PQC License Summary & Excerpts

Background

NIST initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. **Full details can be found in the Post-Quantum Cryptography Standardization page.**

In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere. The goal of *post-quantum cryptography* (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks.

The question of when a large-scale quantum computer will be built is a complicated one. While in the past it was less clear that large quantum computers are a physical possibility, many scientists now believe it to be merely a significant engineering challenge. Some engineers even predict that within the next twenty or so years sufficiently large quantum computers will be built to break essentially all public key schemes currently in use. Historically, it has taken almost two decades to deploy our modern public key cryptography infrastructure.

PROJECT LINKS

ADDITIONAL PAGES

An official website of the United States government Here's how you know

NIST

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Migration to Post-Quantum Cryptography

The advent of quantum computing technology will compromise many of the current cryptographic algorithms, especially public-key cryptography, which is widely used to protect digital information. Most algorithms on which we depend are used worldwide in components of many different communications, processing, and storage systems. Once access to practical quantum computers becomes available, all public-key algorithms and associated protocols will be vulnerable to criminals, competitors, and other adversaries. It is critical to begin planning for the replacement of hardware, software, and services that use public-key algorithms now so that information is protected from future attacks.

https://csrc.nist.gov/projects/post-quantum-cryptography
https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

TLP:CLEAR

QUANTUM-READINESS: MIGRATION TO POST-QUANTUM CRYPTOGRAPHY

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

BACKGROUND

The Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the National Institute of Standards and Technology (NIST) created this factsheet to inform organizations — especially those that support Critical Infrastructure — about the impacts of quantum capabilities, and to encourage the early planning for migration to post-quantum cryptographic standards by developing a Quantum-Readiness Roadmap. NIST is working to publish the first set of post-quantum cryptographic (PQC) standards, to be released in 2024, to protect against future, potentially adversarial, cryptanalytically-relevant quantum computer (CRQC) capabilities. A CRQC would have the potential to break public-key systems (sometimes referred to as asymmetric cryptography) that are used to protect information systems today.

WHY PREPARE NOW?

A successful post-quantum cryptography migration will take time to plan and conduct. CISA, NSA, and NIST urge organizations to begin preparing now by creating quantum-readiness roadmaps, conducting inventories, applying risk assessments and analysis, and engaging vendors. Early planning is necessary as cyber threat actors could be targeting data today that would still require protection in the future (or in other words, has a long secrecy lifetime), using a catch now, break later or harvest now, decrypt later operation. Many of the cryptographic products, protocols, and services used today that rely on public key algorithms (e.g., Rivest-Shamir-Adleman [RSA], Elliptic Curve Diffie-Hellman [ECDH], and Elliptic Curve Digital Signature Algorithm [ECDSA]) will need to be updated, replaced, or significantly altered to employ quantum-resistant PQC algorithms, to protect against this future threat. Organizations are encouraged to proactively prepare for future migration to products implementing the post-quantum cryptographic standards. This includes engaging with vendors around their quantum-readiness roadmap and actively implementing thoughtful, deliberate measures within their organizations to reduce the risks posed by a CRQC.

ETSI TR 103 619 V1.1.1 (2020-07)

CYBER;
Migration strategies and recommendations to Quantum Safe schemes

ANSSI | Agence nationale de la sécurité des systèmes d'information

CONTACTS NEWS

MISSIONS ORGANISATION CYBERSECURITY IN FRANCE SCIENTIFIC STANDING REGULATION SECURITY VISA PUBLICATIONS DIGITAL RISK MANAGEMENT

SCIENTIFIC STANDING > TECHNICAL POSITION PAPERS

FOLLOW UP POSITION PAPER ON POST-QUANTUM CRYPTOGRAPHY

National Cyber Security Centre

ABOUT NCSC CISP

Home Information for... Advice & guidance Education & skills Products & services

Home

WHITEPAPER

Preparing for Quantum-Safe Cryptography

An NCSC whitepaper about mitigating the threat to cryptography from development in Quantum Computing.

National Cyber Security Centre

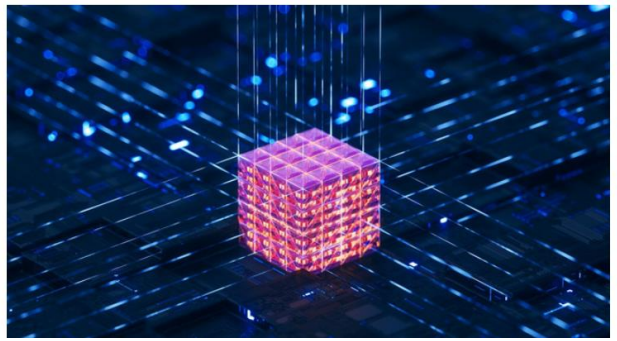
ABOUT NCSC CISP REPORT

Home Information for... Advice & guidance Education & skills Products & services News,

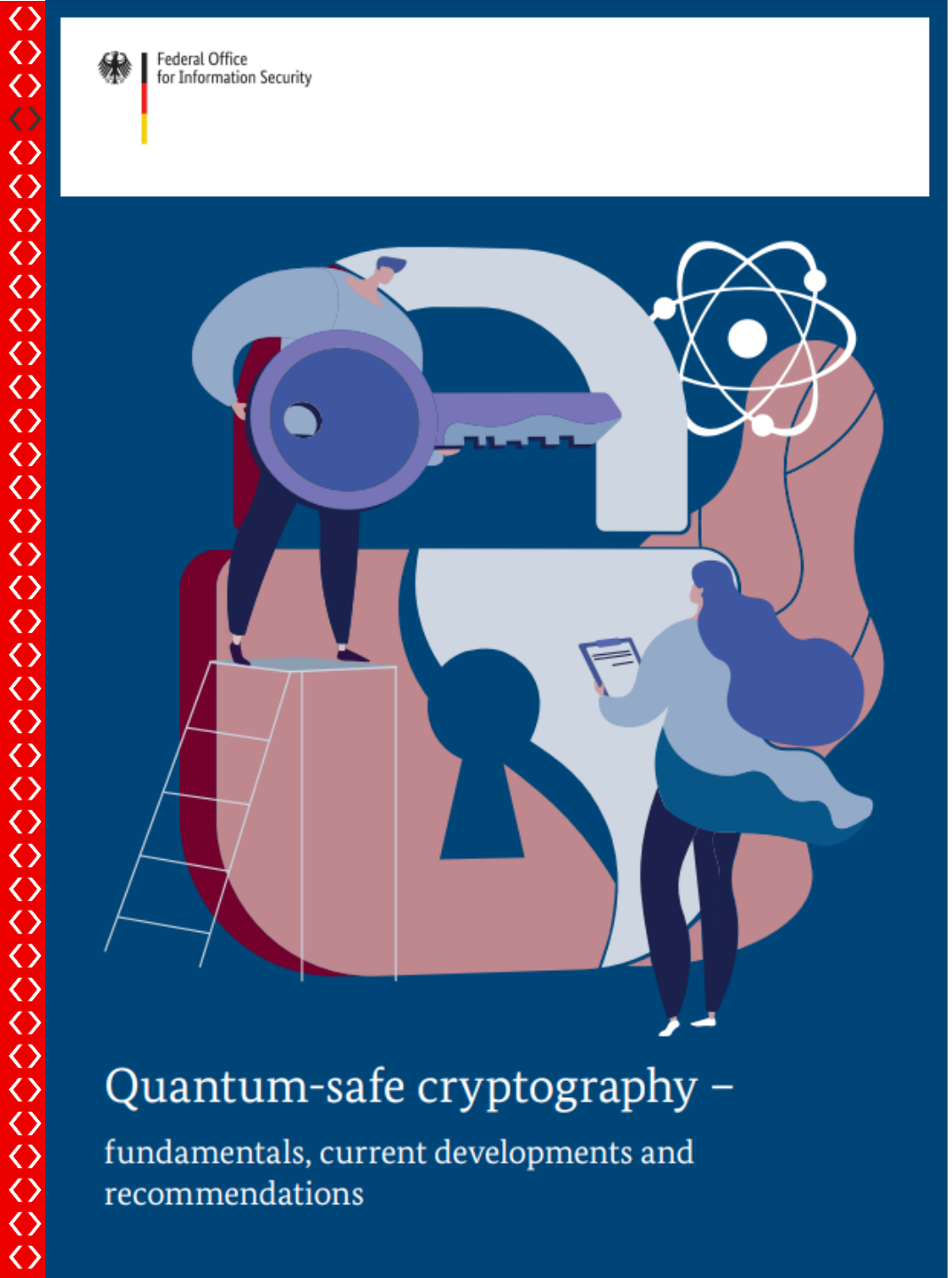
BLOG POST

Next steps in migrating to post-quantum cryptography

New guidance from the NCSC helps system and risk owners plan their migration to post-quantum cryptography (PQC).



https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf
https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography
https://www.ncsc.gov.uk/blog-post/migrating-to-post-quantum-cryptography-pqc
https://www.ssi.gouv.fr/en/publication/anssi-views-on-the-post-quantum-cryptography-transition-2/
https://media.defense.gov/2023/Aug/21/2003284212/-1/-1/0/CSI-QUANTUM-READINESS.PDF



Recommended read for a comprehensive overview

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html

MUST read!

Canadian National Quantum-Readiness

BEST PRACTICES AND GUIDELINES

Version 03 - June 12, 2023

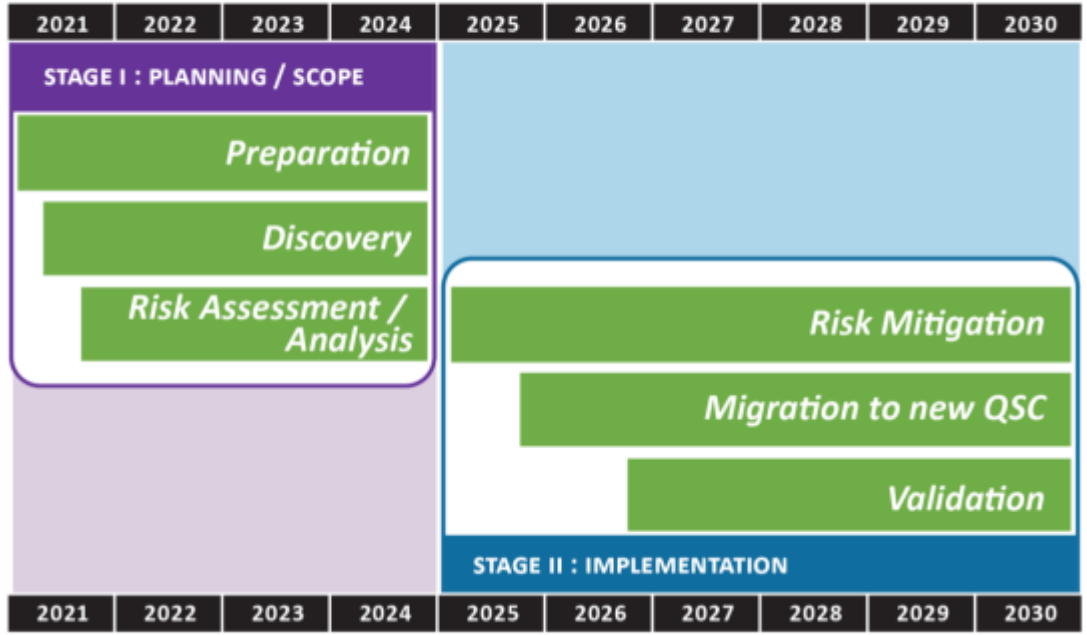
Authored by:

Quantum-Readiness Working Group (QRWG)
of the Canadian Forum for Digital Infrastructure Resilience (CFDIR)

TLP:CLEAR

Quantum-Readiness Program Timeline

Recommendations as of June 2023



https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/attachments/2023/cfdir-quantum-readiness-best-practices-v03.pdf

Canadian National Quantum-Readiness

BEST PRACTICES AND GUIDELINES

Version 03 - June 12, 2023

Authored by:

Quantum-Readiness Working Group (QRWG)
of the Canadian Forum for Digital Infrastructure Resilience (CFDIR)

TLP:CLEAR

ANNEXES:

APPENDICES:

https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/attachments/2023/cfdir-quantum-readiness-best-practices-v03.pdf

Canadian National Quantum-Readiness

BEST PRACTICES AND GUIDELINES

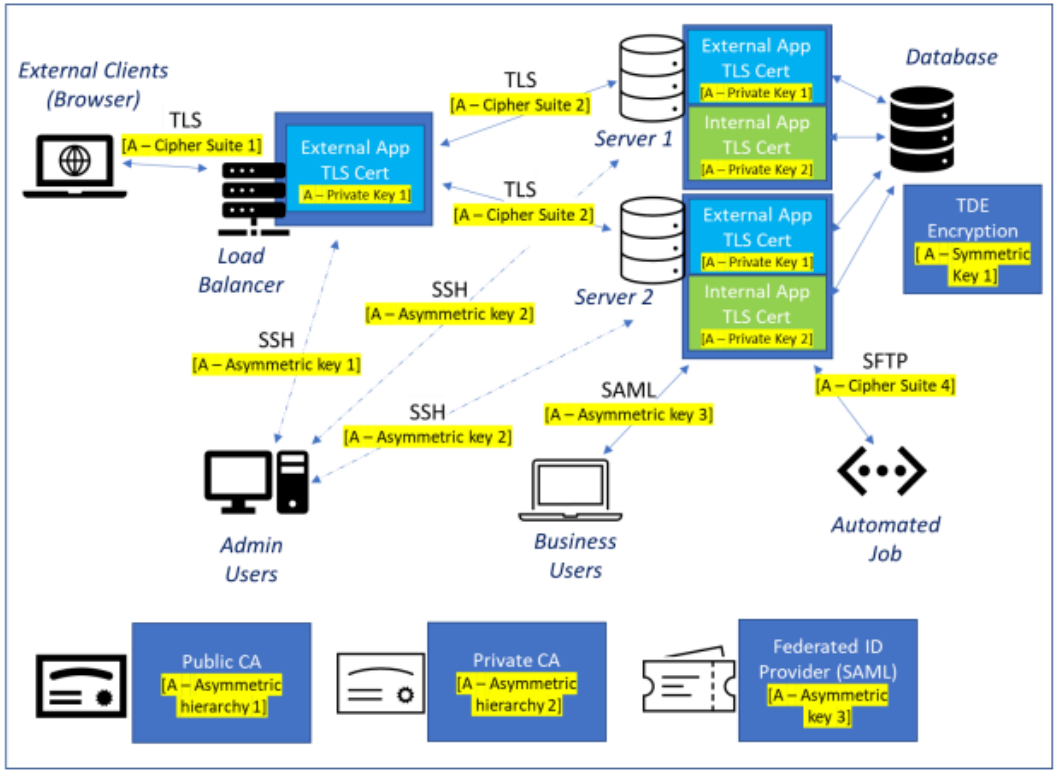
Version 03 - June 12, 2023

Authored by:

Quantum-Readiness Working Group (QRWG)
of the Canadian Forum for Digital Infrastructure Resilience (CFDIR)

TLP:CLEAR

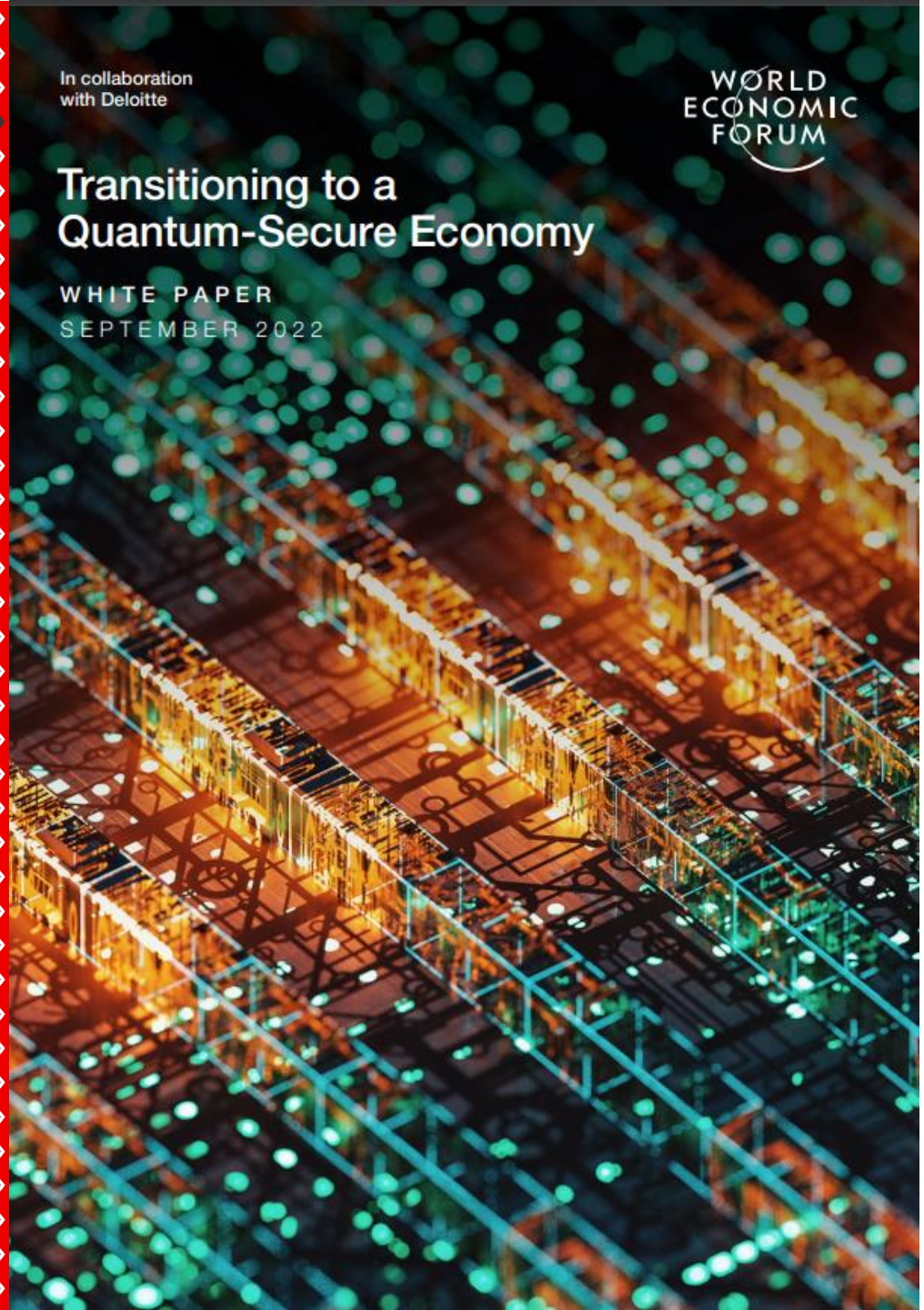
ANNEX I: CRYPTOGRAPHIC-AGILITY EXERCISE NOTES



Notes:

1. The cryptography locations are highlighted in yellow. The goal is to change only these.
2. This is the "before" picture. An equivalent "after" picture is needed.
3. Public Certificate Authority (CA), Private CA, and Federated Identity (ID) Provider are enterprise services used by other systems.
4. The external application uses the public CA and the internal app uses the private CA.
5. The Federated ID Provider provides access for the business users to the internal app.
6. Administrative users can SSH into any box or 'appliance'.

https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/attachments/2023/cfdir-quantum-readiness-best-practices-v03.pdf



1 Define

Quantum security vision (see Fig. 7)

Enable organizations to transition to quantum-secure ecosystems and mitigate quantum threats

2 Identify

Drivers for change (see Fig. 8)

1 Quantum threat materialization ↔ 2 Regulatory pressures ↔ 3 Market dynamics ↔ 4 Cryptography management needs

3 Plan

Quantum security roadmap

Talent & education (see Fig. 9)	**Governance & processes** (see Fig. 10)	**Technology & infrastructure** (see Fig. 11)		
Knowledge pool	Executive support	Post-quantum cryptography	Quantum key distribution	Random number generation
Culture & socialization	Vision & roadmap	Product security		
Training & awareness	Cryptography champions	Enterprise security		
	Policies & standards	Third-party security		

4 Execute

Key factors for success (see Fig. 12)

Standards and certifications | Ecosystem cooperation | Technological innovation & research | Sustainable business & long-term investments

https://www.weforum.org/publications/transitioning-to-a-quantum-secure-economy

FS-ISAC

Preparing for a Post-Quantum World by Managing Cryptographic Risk

Prepared by

FS-ISAC's Post-Quantum Cryptography Working Group

March 2023

1 FS-ISAC

Post-Quantum Cryptography (PQC) Working Group

Risk Model Technical Paper

2 FS-ISAC

Post-Quantum Cryptography (PQC) Working Group

Infrastructure Inventory Technical Paper

3 FS-ISAC

Post-Quantum Cryptography (PQC) Working Group

Current State (Crypto Agility) Technical Paper

4 FS-ISAC

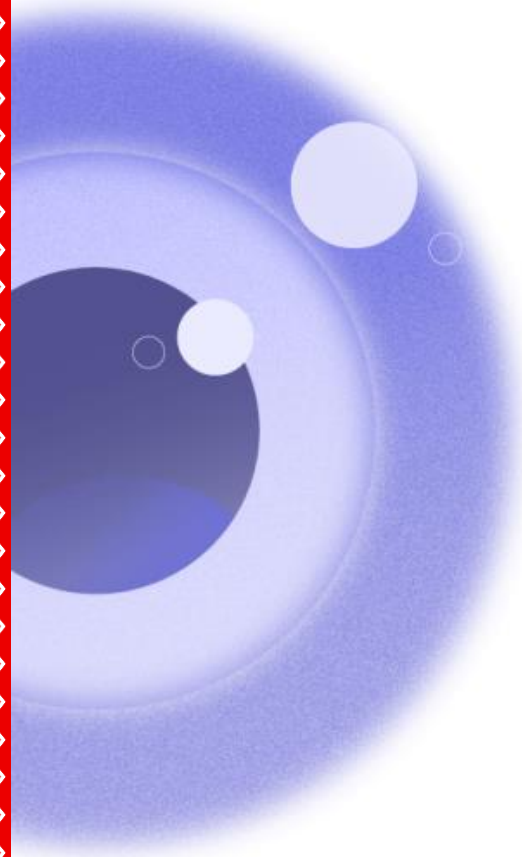
Post-Quantum Cryptography (PQC) Working Group

Future State Technical Paper

https://www.fsisac.com/knowledge/pqc

FS-ISAC

Preparing for a Post-Quantum World by Managing Cryptographic Risk



Prepared by

FS-ISAC's Post-Quantum Cryptography Working Group

March 2023

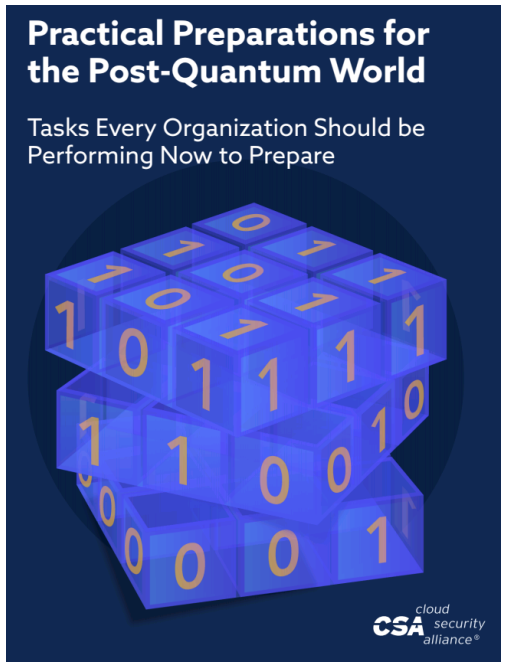
A ROADMAP FOR POST-QUANTUM PREPARATION

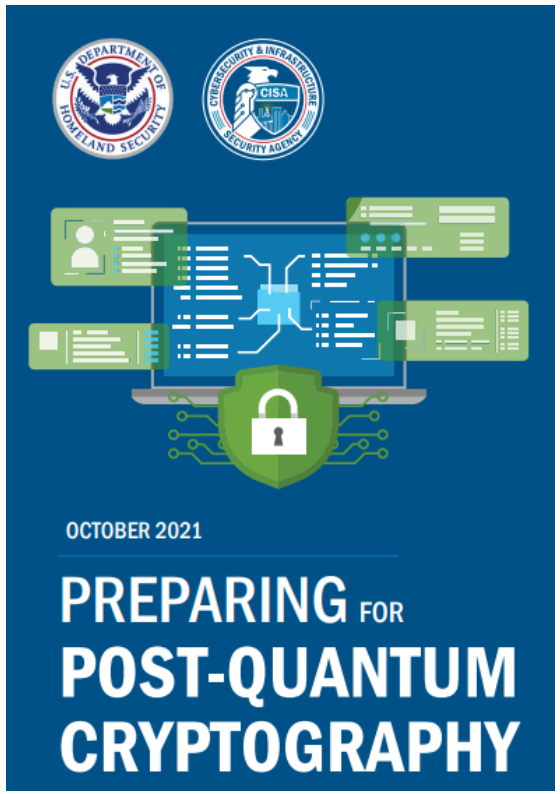
Discovery	I. INVENTORY EXISTING ENCRYPTION ASSETS
	II. ASSESS RISK
Assessment	III. ASSESS VENDORS
	IV. CREATE A RISK ASSESSMENT FRAMEWORK
Modelling	V. APPLY A RISK MODEL
Remediation	VI. REMEDIATION

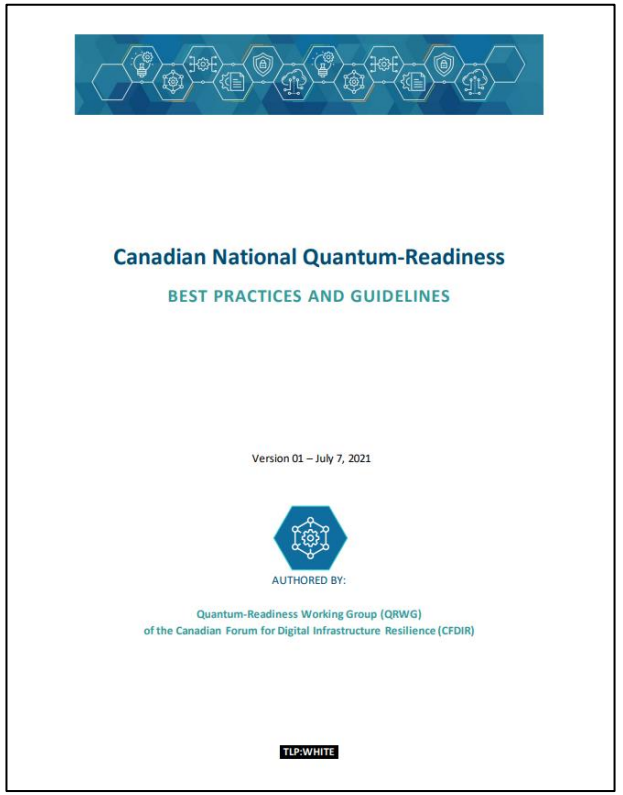
https://www.fsisac.com/knowledge/pqc

Image generated with Bing

What we did







https://cloudsecurityalliance.org/artifacts/practical-preparations-for-the-post-quantum-world/
https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf
https://www.dhs.gov/quantum
https://www.weforum.org/whitepapers/transitioning-to-a-quantum-secure-economy
https://quantum-safe.ca/wp-content/uploads/2022/01/CFDIR-Prati-Tech-Quant-EN.pdf

Proposals for a migration program

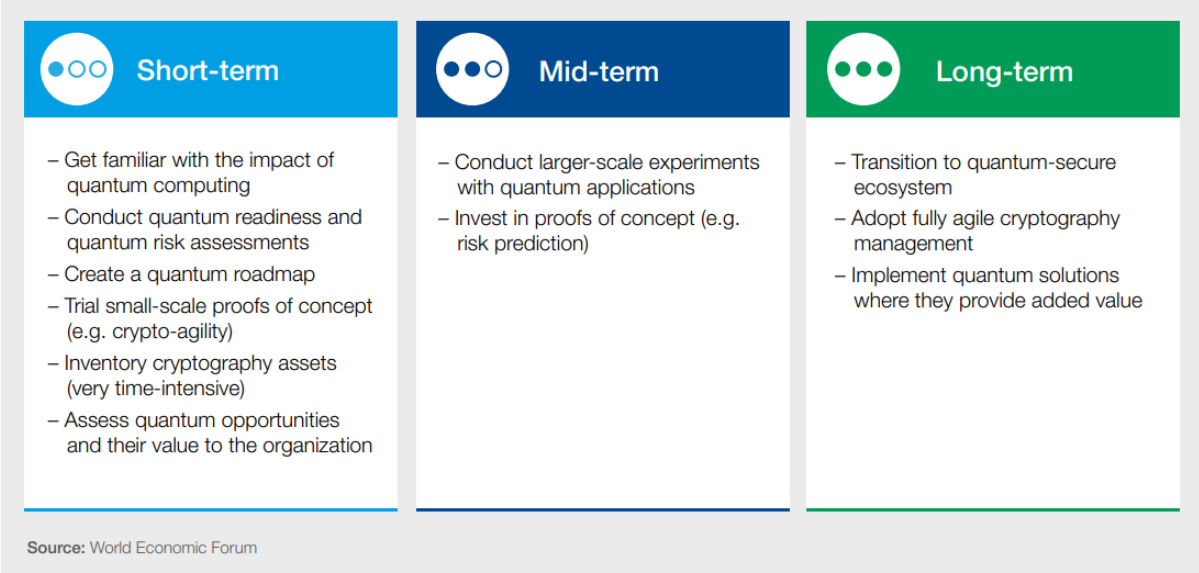
CSA	Education and Awareness	Create Post-Quantum Project	Take data protection inventory	Analysis	Implement Post-Quantum mitigations	
ETSI	Inventory compilation		Preparation of the mitigation plan		Mitigation execution	
DHS	Awareness	Data inventory	Systems inventory	Updating regulations	Preparation for the transition	Transition plan
WEF	Define		Identify	Plan	Execute	
CFDIR	Preparation	Discovery	Risk Assessment		Risk Mitigation	Migration	Validation
FSISAC	Discovery	Assess risk	Assess vendors	Create a risk assessment framework	Apply a risk model	Remediation

The goals

Santander Quantum Threat Program

Santander Quantum Threat Program

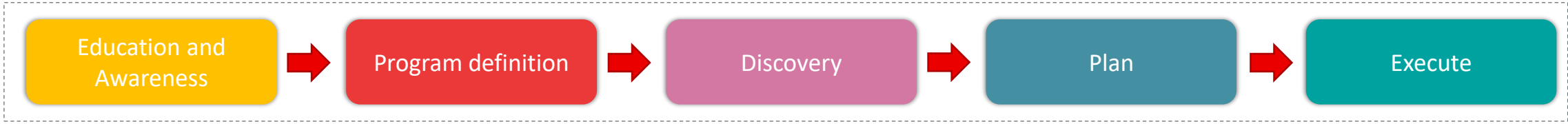
- Santander as a quantum-safe enterprise
- A smooth and efficient transition to quantum-safe cryptography
- A cryptoagile approach to minimize future impacts



In line with recommendation from main agencies and leaders

The phases

Santander Quantum Threat Program



Phases	Main Goal	Relevant Tasks
Education and Awareness	The organization, at all levels, understands the quantum threat, the need for action, and the program. Key stakeholders are identified and engaged.	Train the organization
		Train third parties
		Build a cryptography community
Program Definition	Define the global program strategy and governance model.	Create an initial program plan and timeline
		Create a program team and a program management office
		Identify local stakeholders in business units
		Track external stakeholders (regulations, standards, technologies, partners and vendors)
Discovery	Create the tooling and data management for the program with automation at the core. Identify use cases of cryptography in the Group.	Create the tooling environment to track the usage of cryptography
		Identify the time validity for all protected data
		Generate data-driven insights
Plan	Establish priorities for the different use cases according to a risk-impact evaluation. Define actions to tackle the threats.	Execute a risk analysis of the cryptography use cases
		Design technical solutions for the different use cases
		Define a prioritized list of projects
Execute	Execute the different plans. Track execution success. Feedback lessons learned.	Launch local projects
		Support local execution with expert analysis. Retrieve feedback
		Generate compliance and control reports

Threat dimensions

#1 Confidentiality

- Harvesting of comms data (Harvest now, decrypt later)
- Encrypted storage data (backups)

#2 Authentication

- Recovering authentication private keys
- Creating fake credentials
- Sign malicious code

#3 Legal history

- Recovering signing private keys
- Manipulating signed documents
- Creating fake documents with valid signatures

Santander

Risk based prioritization

Santander Quantum Threat Program

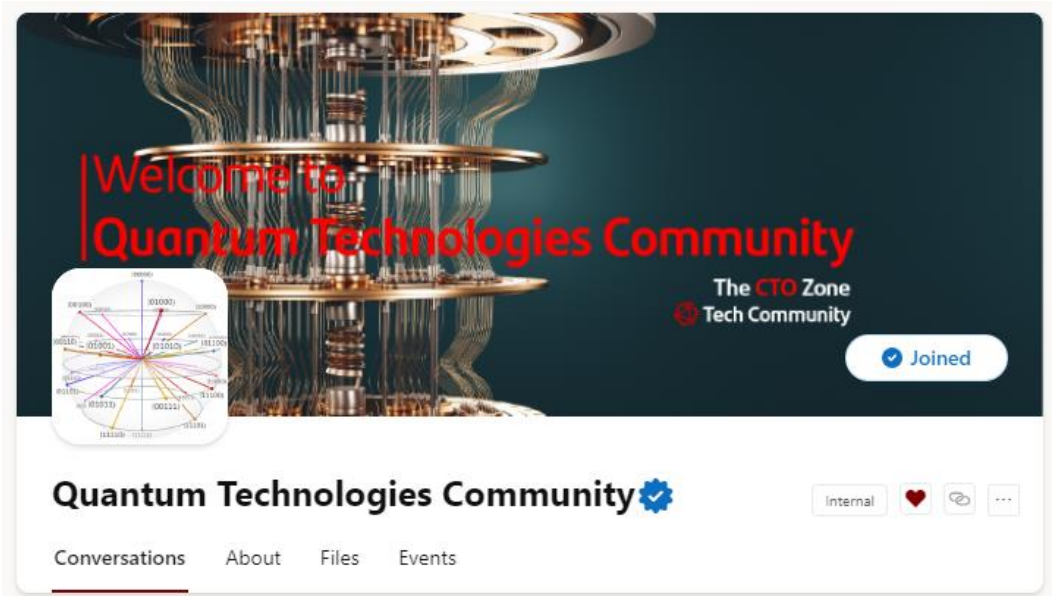
- The Quantum threat to cryptography can impact Santander in different areas and applications. Actions will span a multiyear timeframe (10-15 years) and need to be prioritized.
- Risk-based priotization will ensure that most relevant use cases will be addressed earlier.
- The following table shows how the risk analysis can be executed. The table features minimum feature relevance as 1 and maximum as 5. The risk is evaluated as a multiplication of the value of all features.

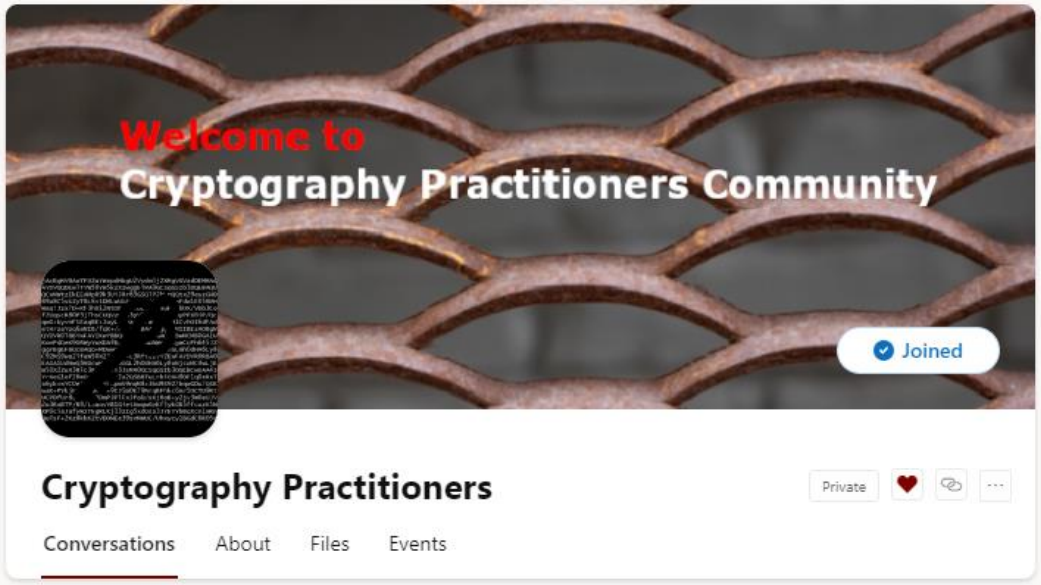
Dimension	Use Case	Time validity	External availability	Sensibility	Risk
Confidentiality	Public websites encryption with TLS	1	5	5	25
	Internal access to servers using SSH	2	1	3	6
	Teleworking using VPNs	3	3	5	45
	Site to site VPNs using IPSEC	5	3	5	75
	Encryption of data at rest on premises (disks, backups...).	5	2	3	30
	Encryption of data at rest in the cloud	5	3	5	75
Authentication	Public digital certificates	2	5	5	50
	Internal digital certificates	2	1	4	8
Legal History	Digital signatures in contracts	5	4	5	100

Create internal communities

Block›chain

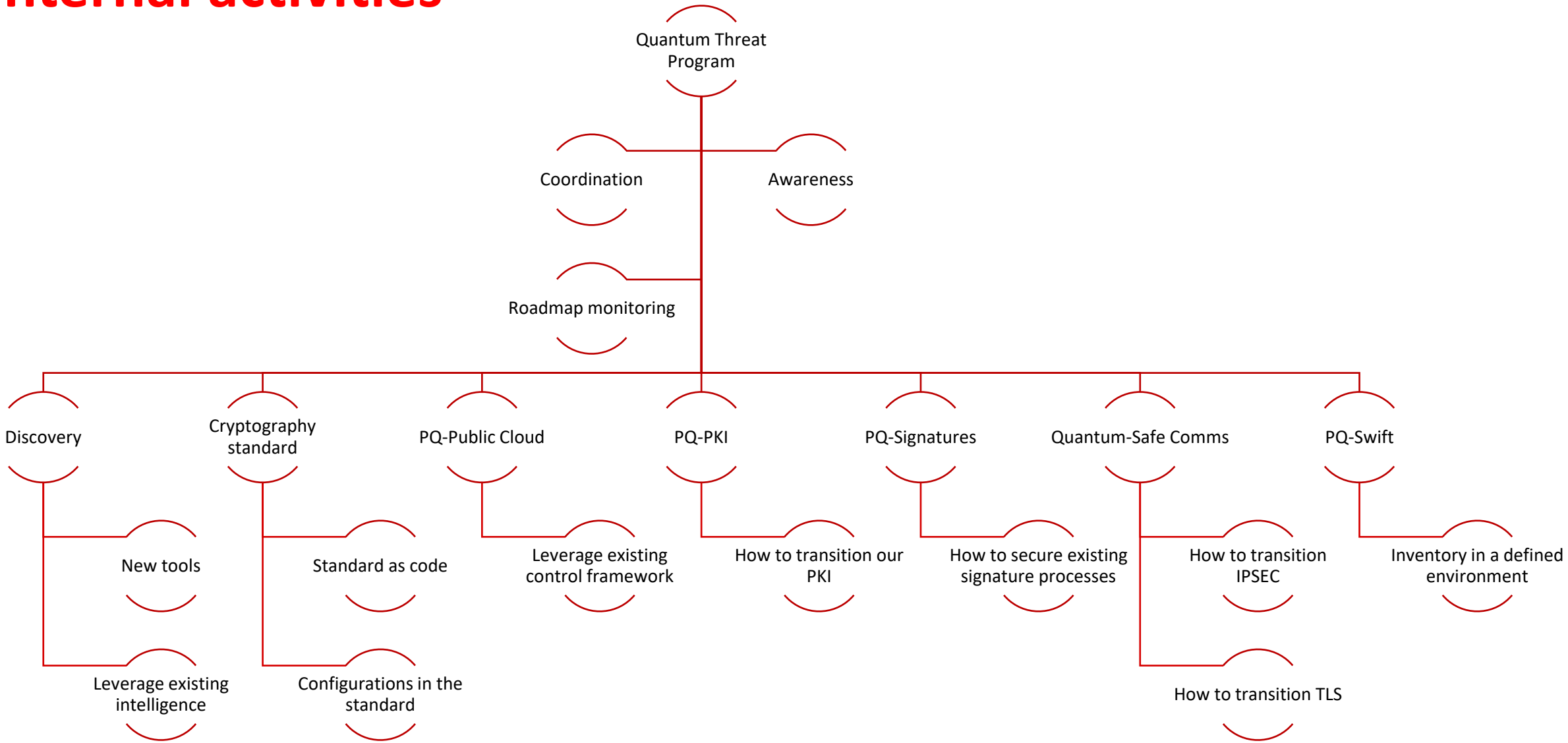
¡JOIN US!



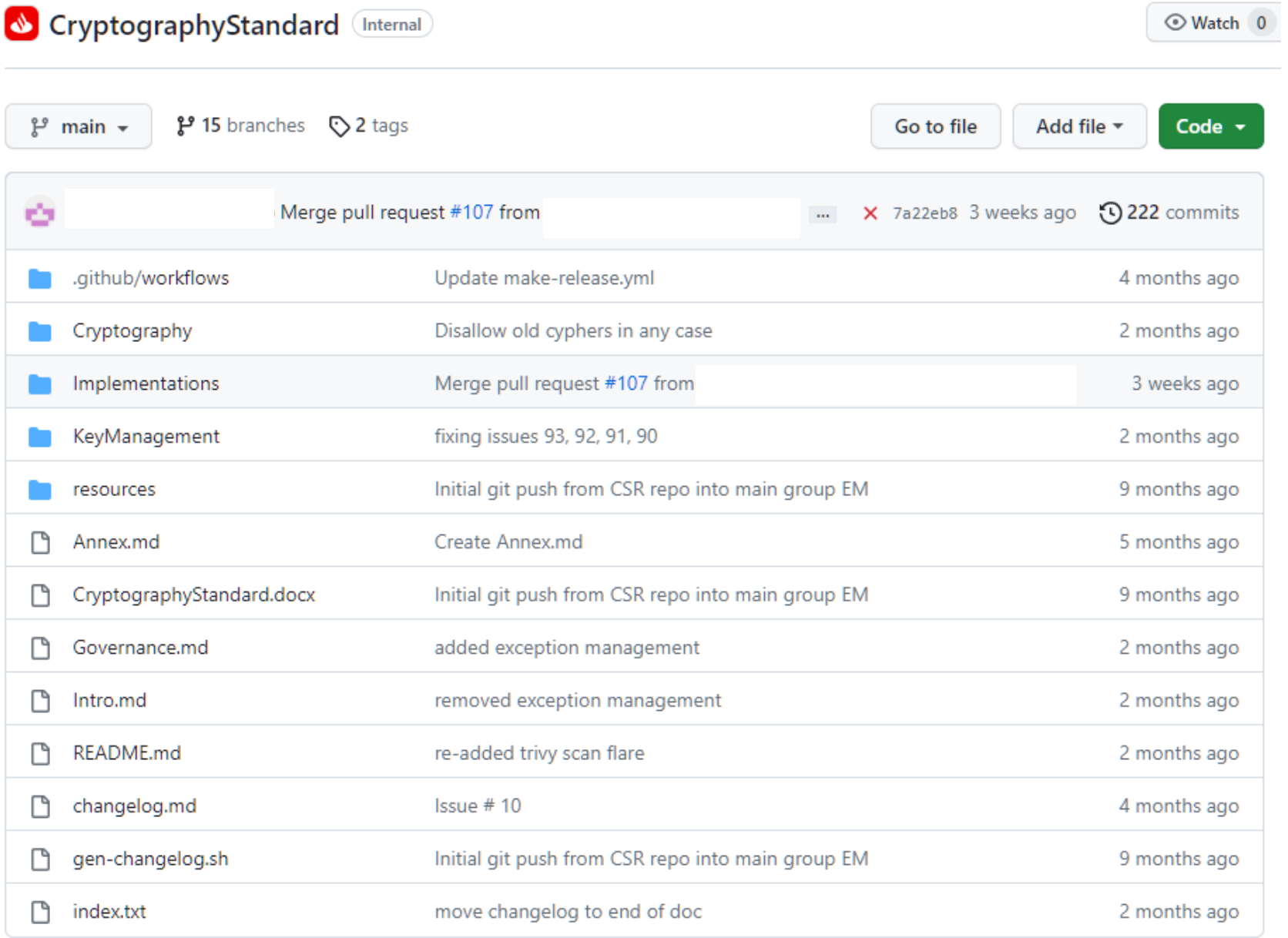


Santander

Internal activities



Cryptoagility begins with agile standards

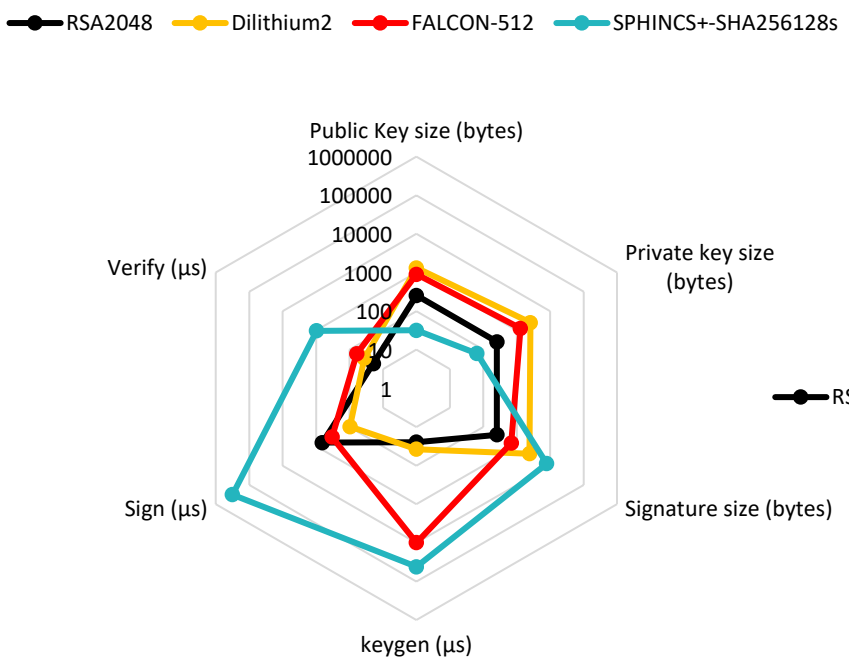


Signature algorithm comparison

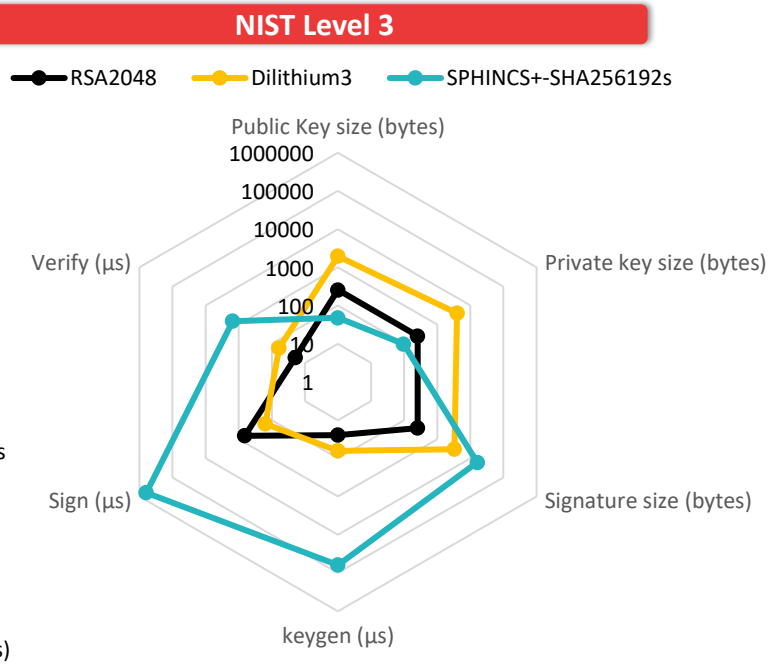
Santander Quantum Threat Program

Low values better

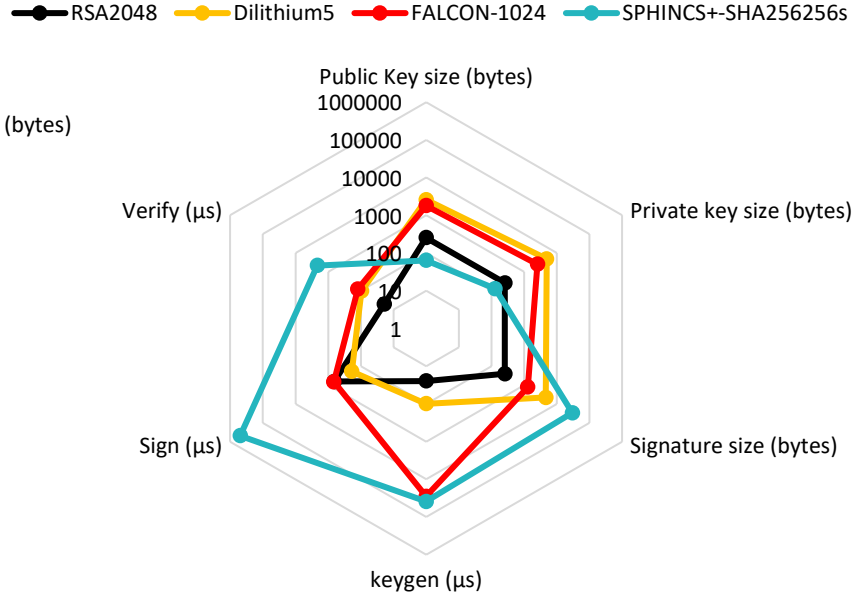
NIST Level 1&2



NIST Level 3



NIST Level 5



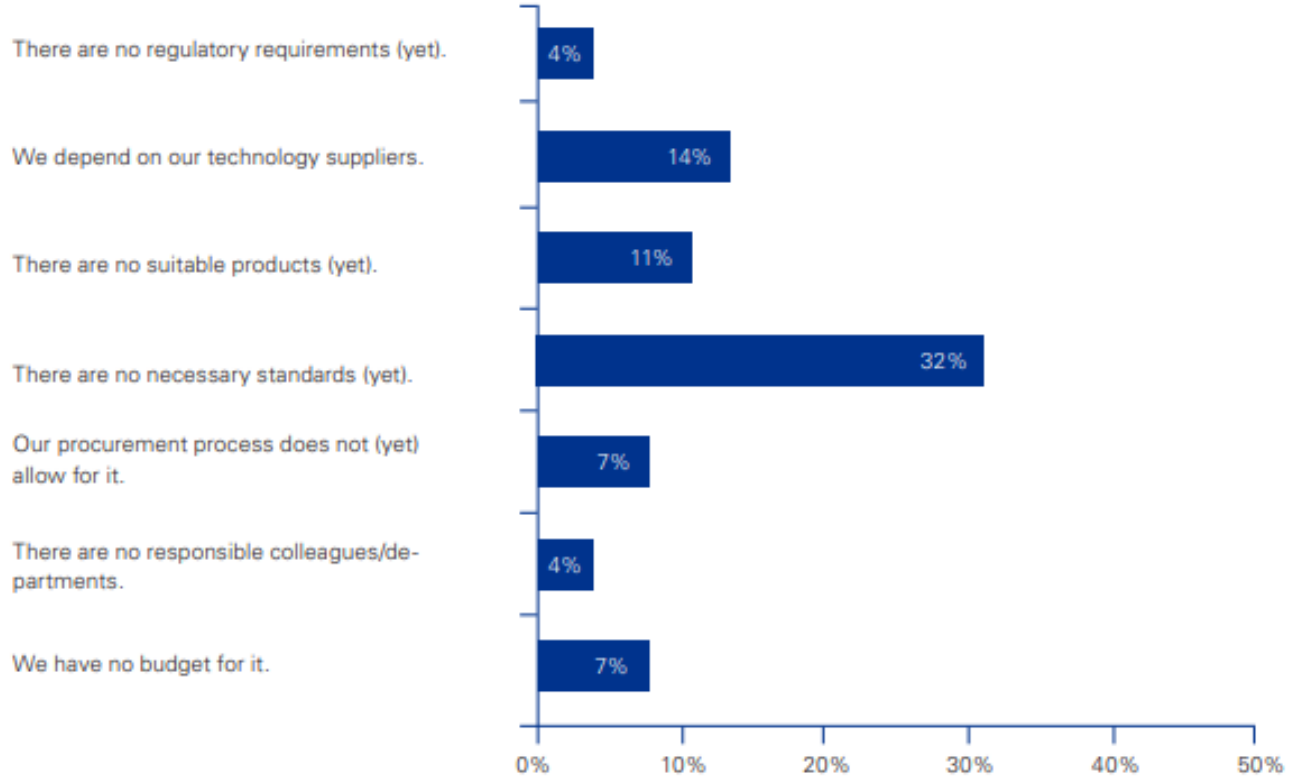
RSA2048 used as a performance reference as it is often used currently.
It's classical security (112 bits) is inferior to Level 1 (128 bits).

KPMG

Federal Office for Information Security

Market Survey on Cryptography and Quantum Computing

Fig. 10: If there are no initiatives/projects regarding this topic in your organization — why not?



https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Marktumfrage_EN_Kryptografie_Quantencomputing.html


I understand the threat, but I can’t engage the organization
We still fight with obsolete software, let alone cryptography
We have little expertise on cryptography
Image generated with Bing

Forbes

FORBES > INNOVATION

The Top Five Priorities For Enterprise CISO In 2023

Ivan Novikov Former Forbes Councils Member
Forbes Technology Council
COUNCIL POST | Membership (Fee-Based)

Jan 11, 2023, 07:30am EST

CEO of Wallarm, API security company.

GETTY

As technology continues to evolve, the role of the chief information security officer (CISO) becomes increasingly important in protecting an organization's

I recently surveyed 25 enterprise CISOs and the following priorities emerged as key focus areas for 2023:

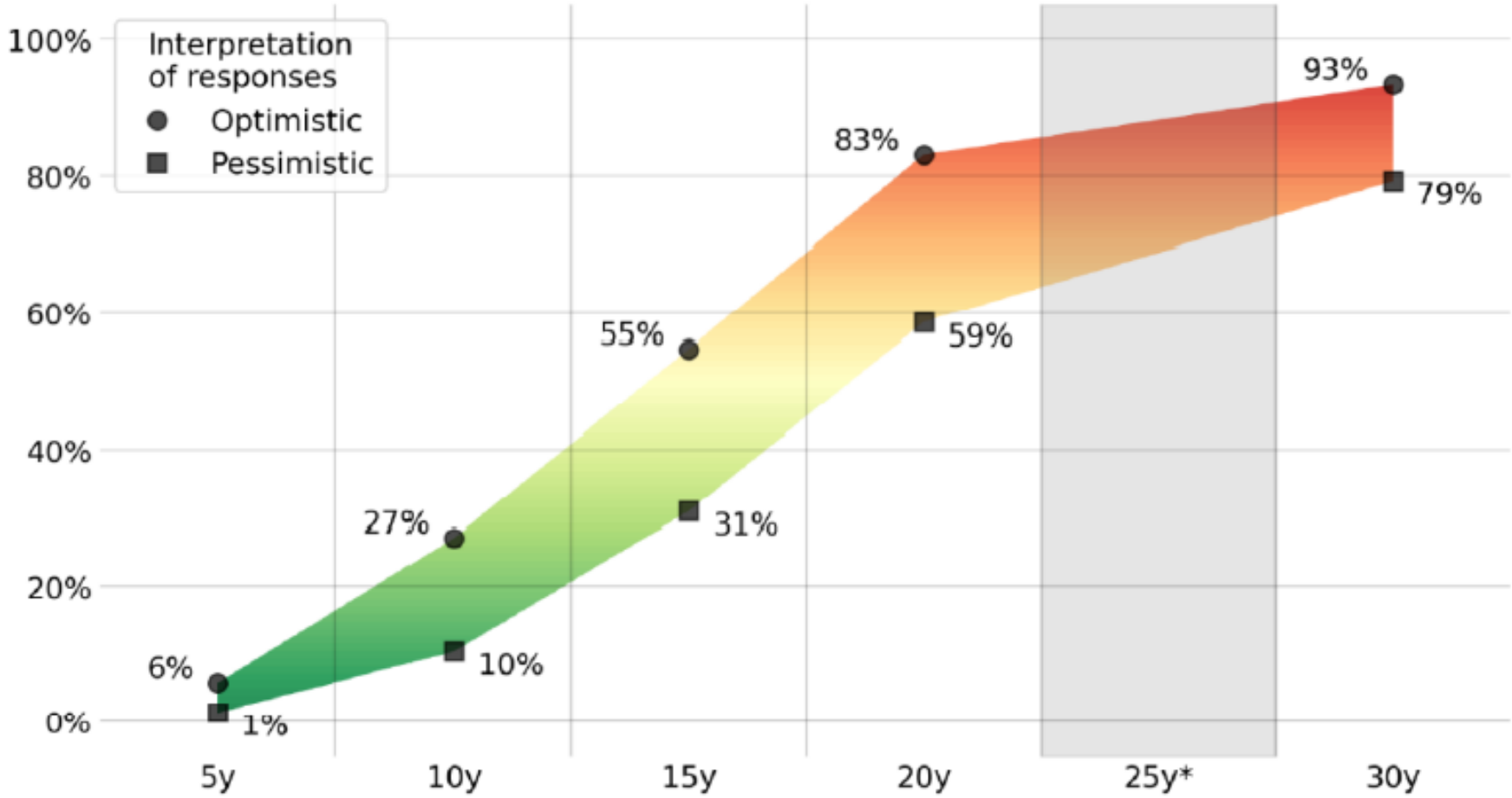
1. **Smart Hiring Among Layoffs**
2. **TCO Focus On Products**
3. **Improve Threat Prevention To Combat Cyber Turbulence**
4. **Infrastructure Optimization Expands Attack Surfaces**
5. **Embracing Automation To Enhance Cybersecurity Measures**

https://www.forbes.com/sites/forbestechcouncil/2023/01/11/the-top-five-priorities-for-enterprise-ciso-in-2023/

Image generated with Bing

2022 OPINION-BASED ESTIMATES OF THE CUMULATIVE PROBABILITY OF A DIGITAL QUANTUM COMPUTER ABLE TO BREAK RSA-2048 IN 24 HOURS, AS FUNCTION OF TIMEFRAME

Estimates of the cumulative probability of a cryptographically-relevant quantum computer in time: range between average of an optimistic (top value) or pessimistic (bottom value) interpretation of the estimates indicated by the respondents.
[*Shaded grey area corresponds to the 25-year period, not considered in the questionnaire.]

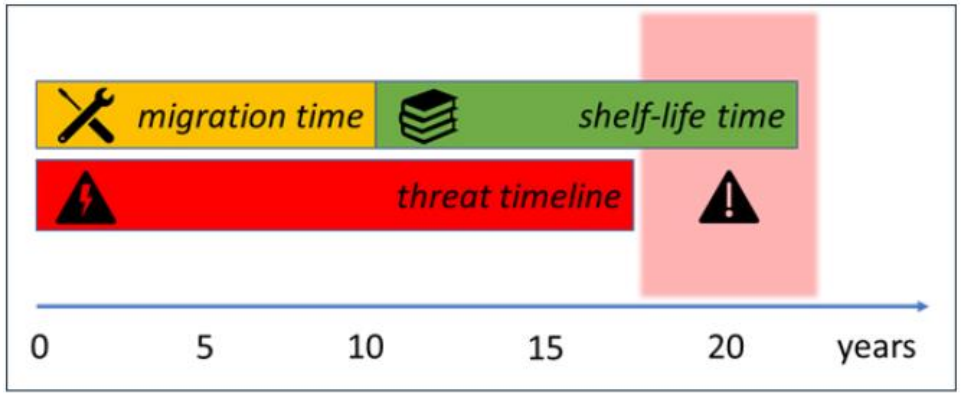


https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/

KPMG

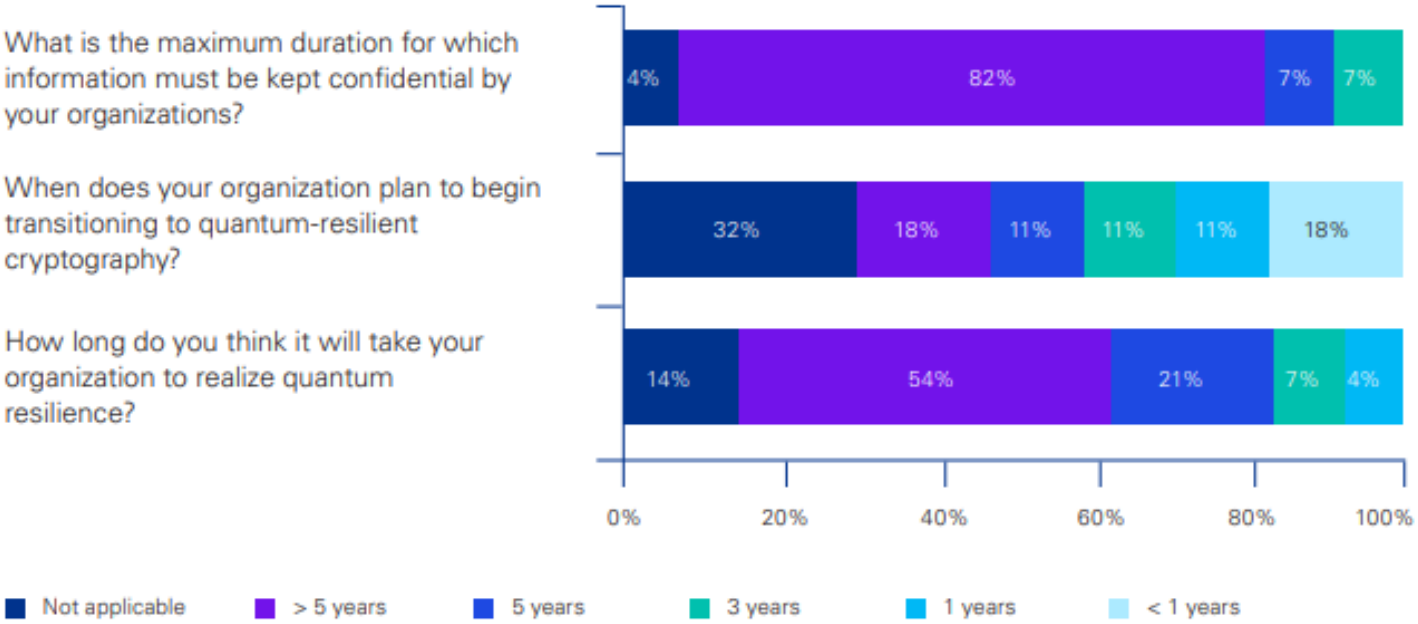
Federal Office for Information Security

Market Survey on Cryptography and Quantum Computing



https://globalriskinstitute.org/publications/quantum-threat-timeline-report-2020/

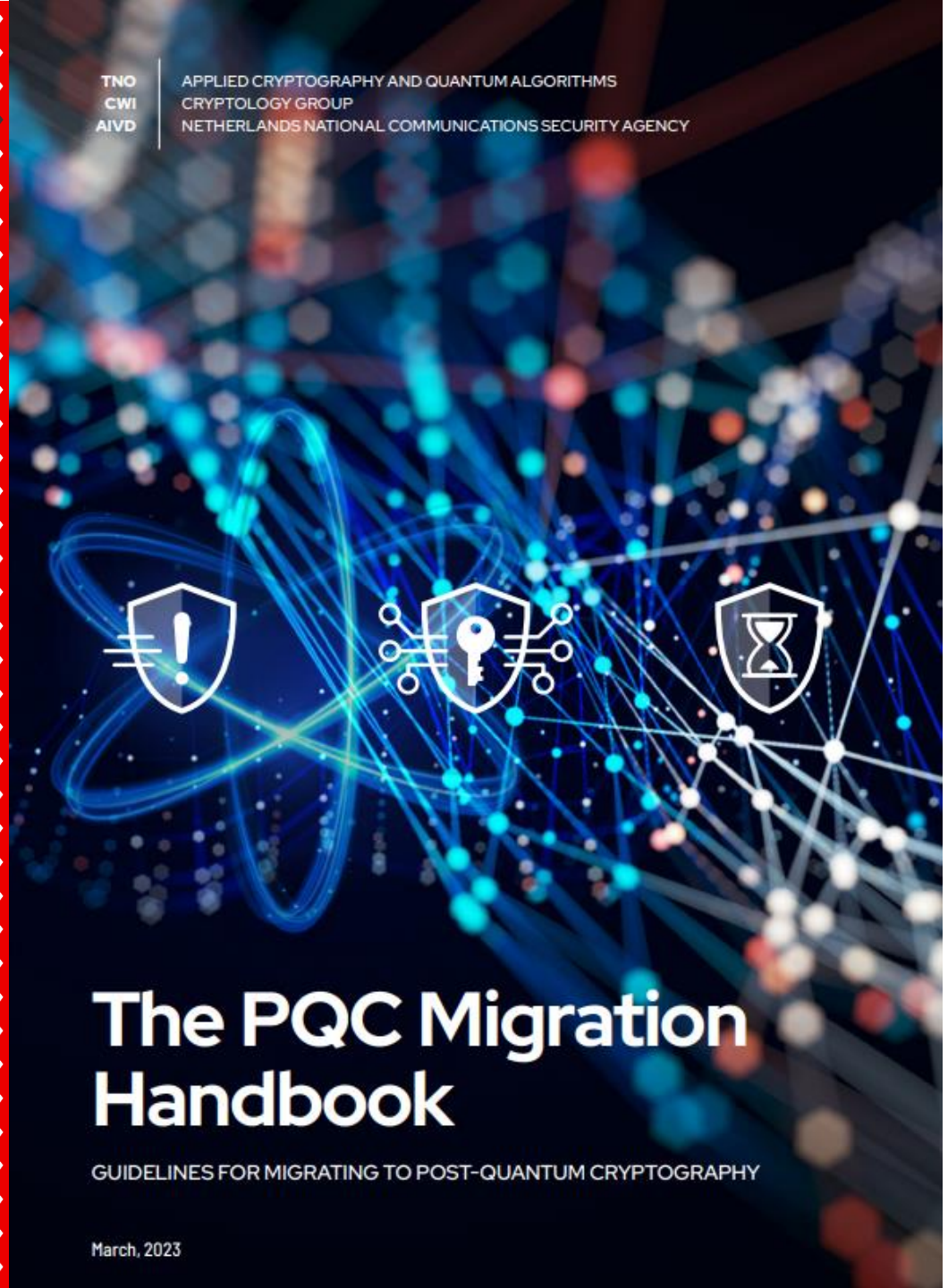
Fig. 7: Please evaluate the following timescales



Source: KPMG in Germany, 2022; figures in percent, Rounding differences possible

¡QUANTUM SAFETY WILL NOT BE ACHIEVED IN TIME BY ANY OF THE SURVEY PARTICIPANTS!

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Marktumfrage_EN_Kryptografie_Quantencomputing.html



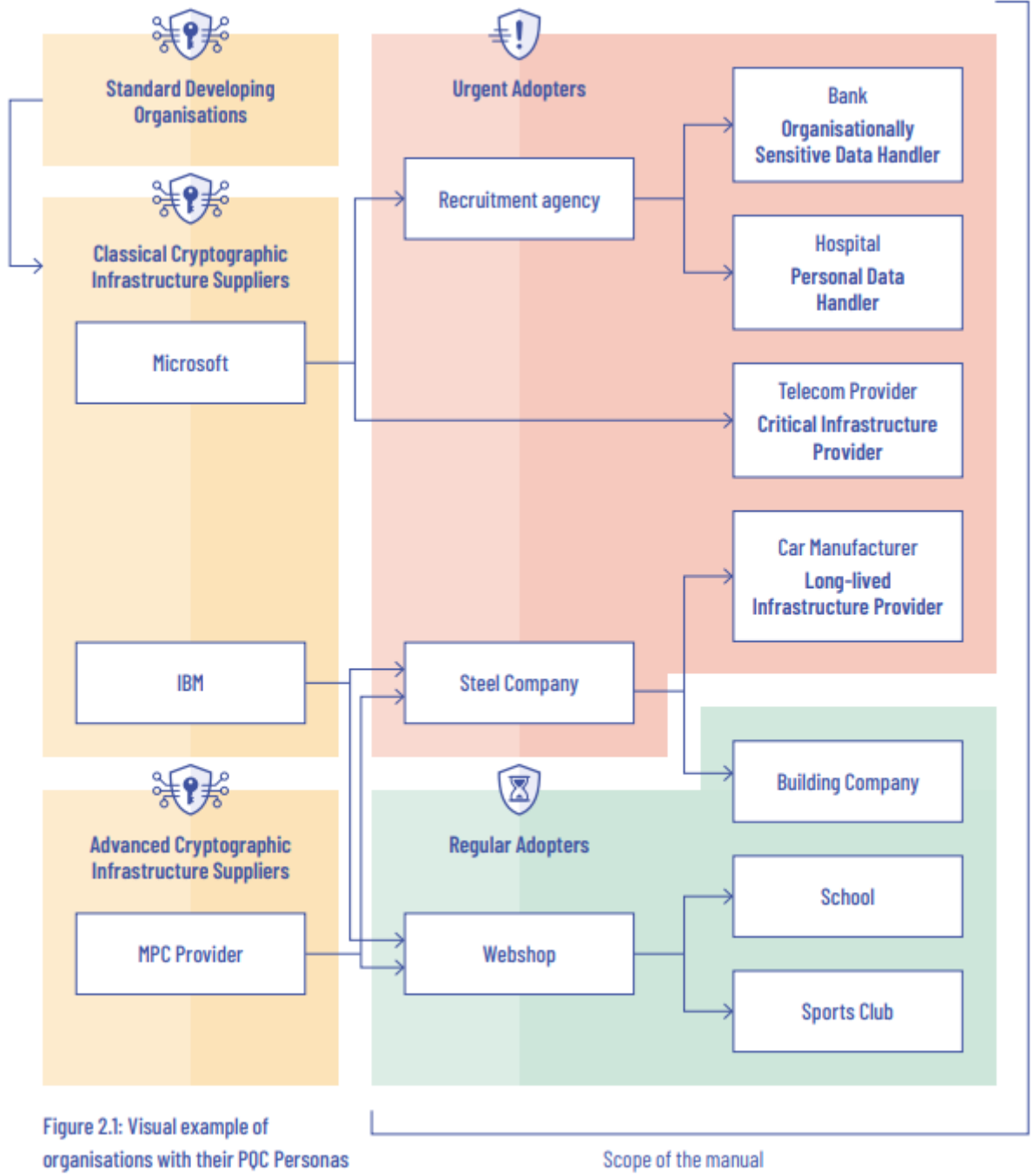


Figure 2.1: Visual example of organisations with their PQC Personas

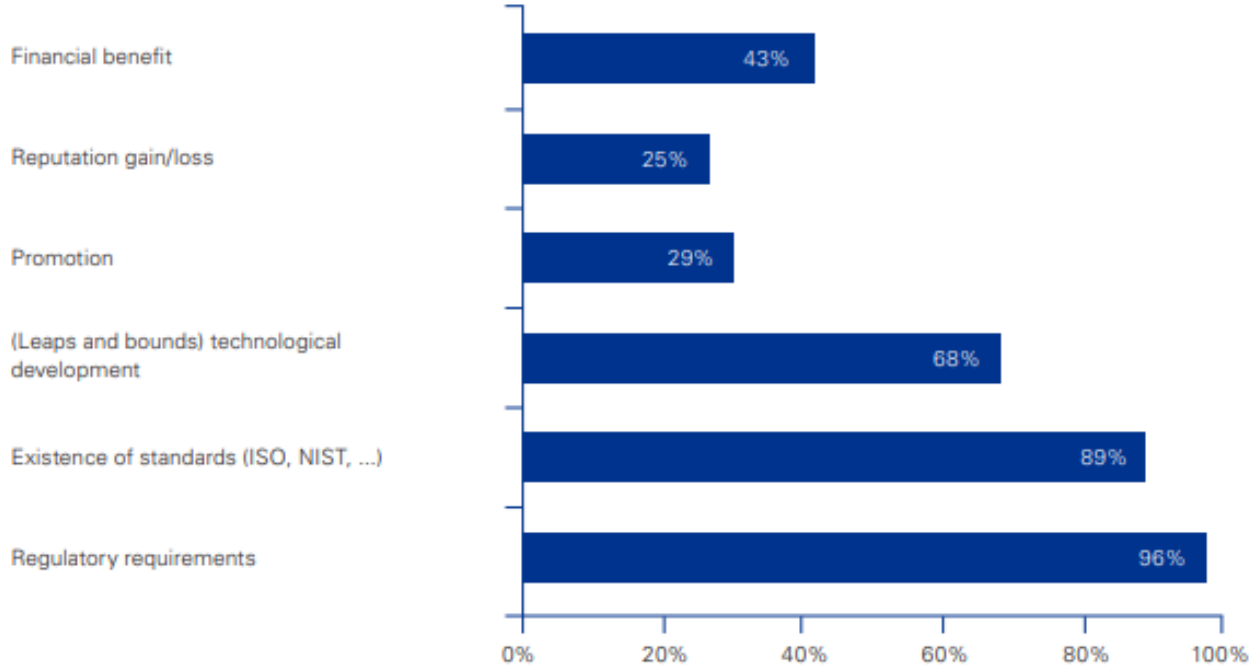
https://english.aivd.nl/publications/publications/2023/04/04/the-pqc-migration-handbook

KPMG

Federal Office for Information Security

Market Survey on Cryptography and Quantum Computing

Fig. 13: What would encourage your organisation to make investment decisions?



https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Marktumfrage_EN_Kryptografie_Quantencomputing.html

USA executive actions

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

November 18, 2022

M-23-02

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Director

SUBJECT: Migrating to Post-Quantum Cryptography

This memorandum provides direction for agencies to comply with National Security Memorandum 10 (NSM-10), *on Promoting United States Leadership in Quantum Computing While Mitigating Risk to Vulnerable Cryptographic Systems* (May 4, 2022).[1]

By May 4, 2023, and annually thereafter until 2035, or as directed by superseding guidance, agencies are directed to submit a prioritized inventory of information systems and assets, excluding national security systems,[7] that contain CRQC-vulnerable cryptographic systems to ONCD and the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA).[8]

Within 30 days of the publication of this memorandum, agencies will designate a cryptographic inventory and migration lead for their organization. Each agency should identify its lead to OMB using the contact information in Section VII. OMB will rely on these designated leads for Government-wide coordination and for engagement on planning and implementation efforts within each organization.

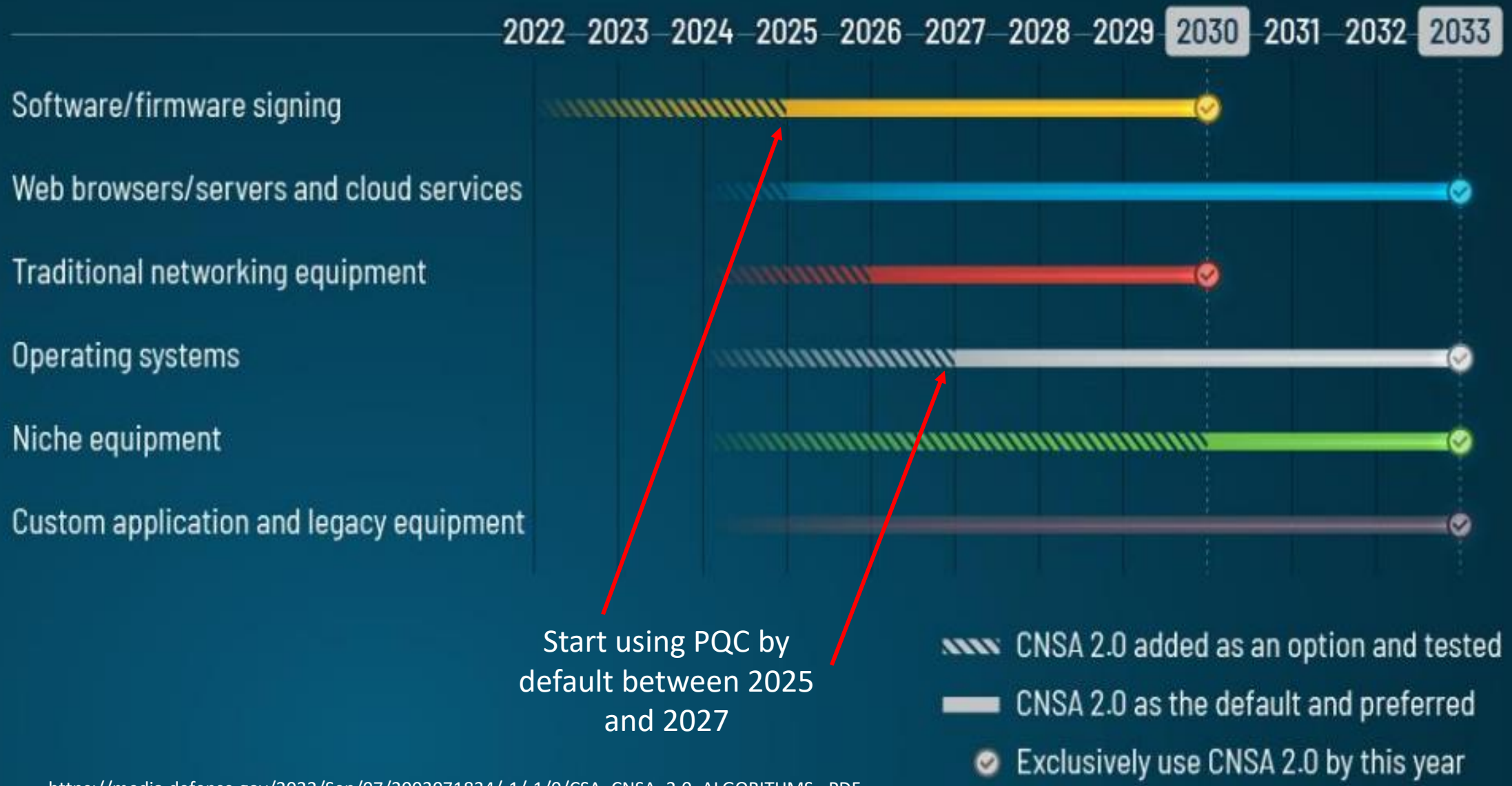
No later than 30 days after the submission of each annual inventory of cryptographic systems required under Section II of this memorandum, agencies are required to submit to ONCD and OMB an assessment of the funding required to migrate information systems and assets inventoried under this memorandum to post-quantum cryptography during the following fiscal year. These agency assessments will inform the funding assessments required by NSM-10 Section 3(c)(iv).

Within one year of the publication of this memorandum, CISA, in coordination with NSA and NIST, will release a strategy on automated tooling and support for the assessment of agency progress towards adoption of PQC.

This strategy is expected to address discovery options for internet-accessible information systems or assets, as well as internal discovery of information systems or assets that are not internet-accessible.

https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf

CNSA 2.0 Timeline



https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

FIGURE 1 | **Guiding principles to understand the quantum-secure transition**

Awareness and engagement

Ensure the organizational governance structure institutionalizes quantum risk

The quantum threat requires organizations to align their governance structure to their quantum cyber readiness transition by defining clear goals, roles and responsibilities and creating leadership buy-in to enforce change effectively.

Raise quantum risk awareness throughout the organization

Demystifying the quantum threat is key. This requires that not only quantum cyber readiness experts but also senior leaders and risk managers understand the risk and impact of the threat to the organization.

Cryptography management

Treat and prioritize quantum risk alongside existing cyber risks

A quantum cyber-ready organization follows a structured approach to evaluate and manage quantum risk and integrates mitigating this risk into existing cyber risk management procedures.

Make strategic decisions for future technology adoption

Managing quantum risk provides organizations with opportunities to reassess their technology landscape, specifically the use of cryptography. To make the most out of technology solutions that help mitigate quantum risk, organizations should make strategic technology decisions that support "crypto-agility" to achieve their security objectives.

Collaboration

Encourage collaboration across ecosystems

Quantum risk is a systemic risk. An effective quantum security strategy includes collaborating and sharing information with other organizations to identify risks throughout the ecosystem and suppliers to jointly mitigate such risks.

https://www.weforum.org/publications/quantum-readiness-toolkit-building-a-quantum-secure-economy/


Image generated with Bing


¡Gracias!

Post-Quantum Cryptography Conference

PKI Consortium

ENTRUST

HID

PQ SHIELD

Fortanix

KEYFACTOR

NOREG

QRL

THALES

d-trust.

amsterdam convention bureau

ascertia

亞洲誠信 TRUSTAsia