Post-Quantum

Cryptography Conference

Quantum-Safety Timelines in the Financial Sector

Jaime Gómez García

Global Head of the Santander Quantum Threat Program, Chair of the Europol Quantum Safe Financial Forum

KEYFACTOR CRYPTO4A SSL.com ENTRUST HID

October 28 - 30, 2025 - Kuala Lumpur, Malaysia

PKI Consortium

Quantum Safety Timelines in the Financial Sector

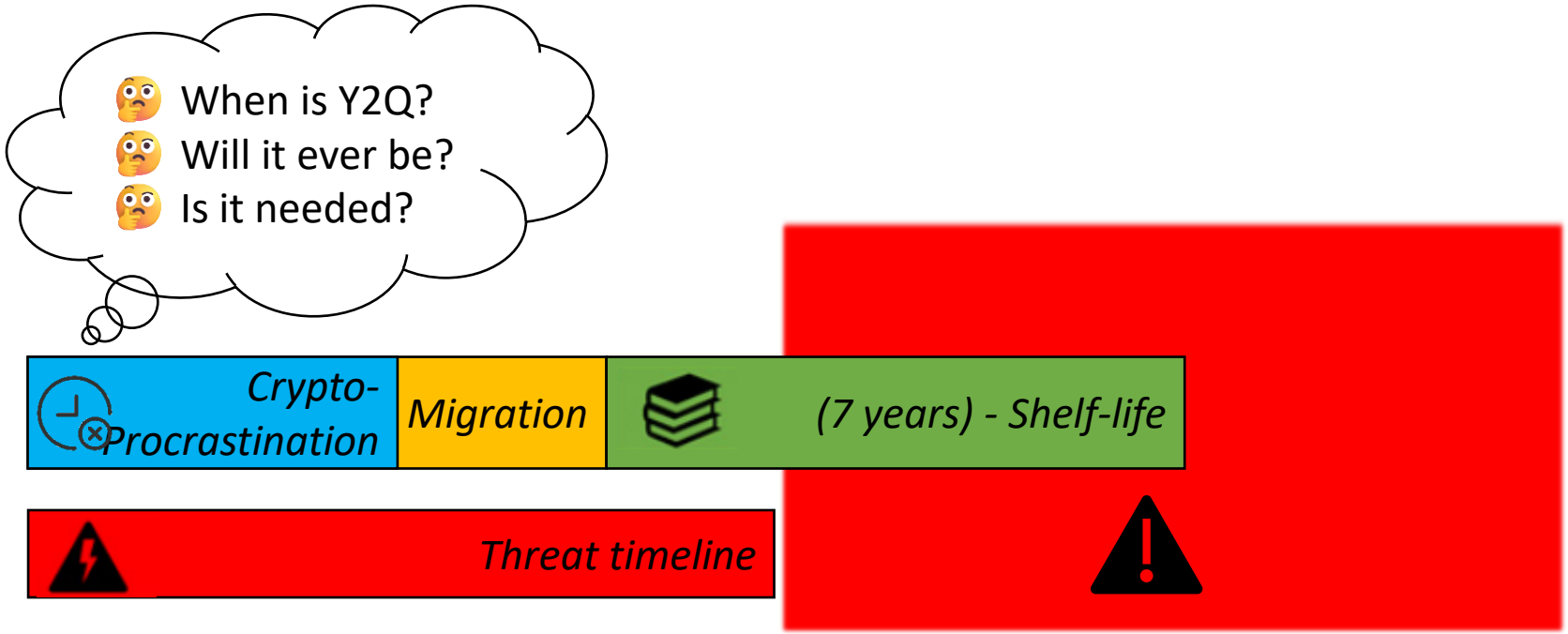
PQC Conference – Kuala Lumpur

Jaime Gómez García

Oct. 29th, 2025

Santander

Augmented Mosca's theorem



End of Life for Vulnerable Cryptography

Not about quantum computers anymore

NIST Internal Report
NIST IR 8547 ipd

Transition to Post-Quantum Cryptography Standards

Initial Public Draft

Dustin Moody
Ray Perlner
Andrew Regenscheid
Angela Robinson
David Cooper

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8547.ipd

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

Table 2: Quantum-vulnerable digital signature algorithms

Digital Signature Algorithm Family	Parameters	Transition
ECDSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
EdDSA [FIPS186]	≥ 128 bits of security strength	***Disallowed*** after 2035
RSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035

4.1.2. Key Establishment

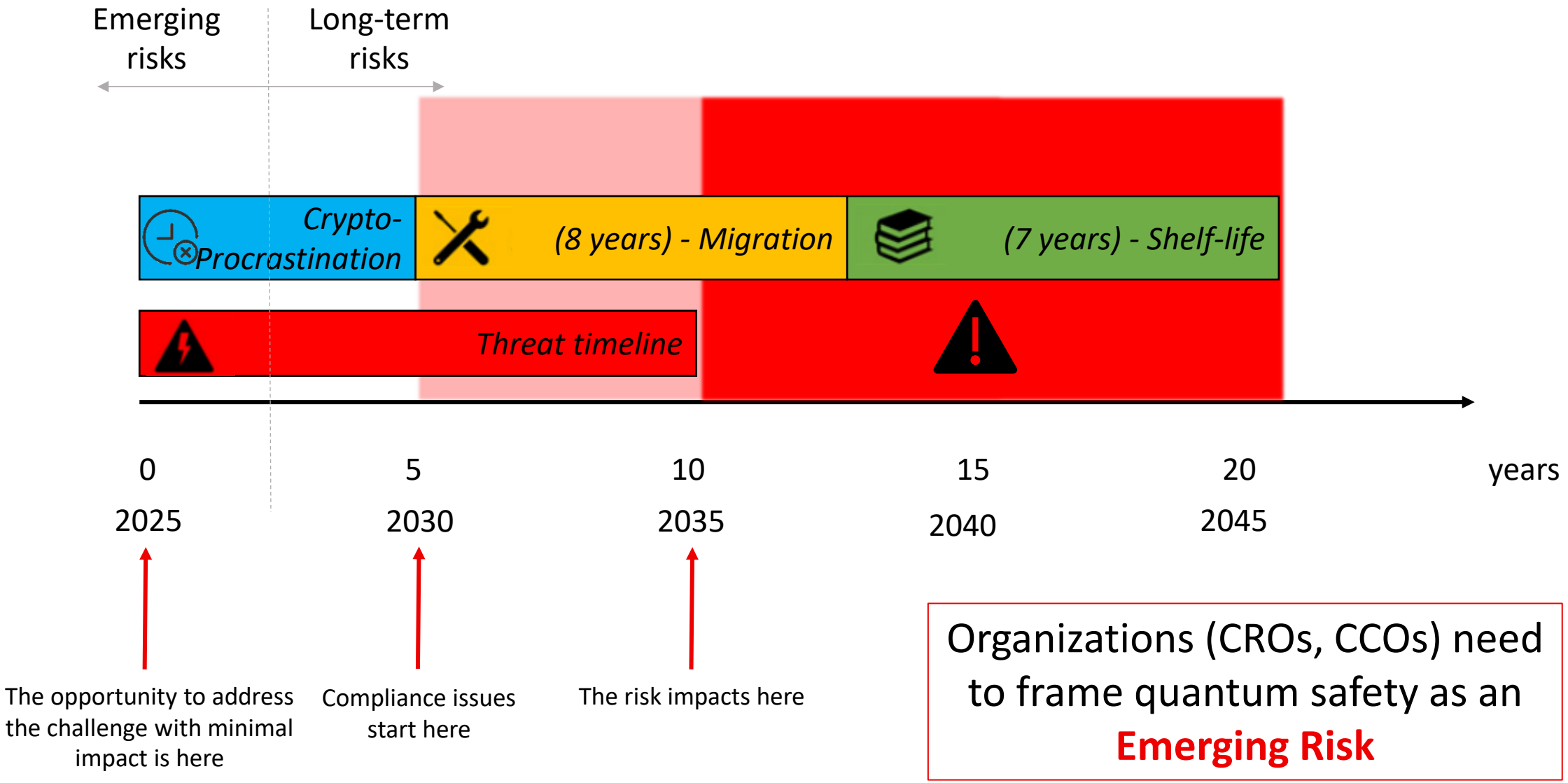
Table 4 lists currently approved quantum-vulnerable key-establishment.

Table 4: Quantum-vulnerable key-establishment schemes

Key Establishment Scheme	Parameters	Transition
Finite Field DH and MQV [SP80056A]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
Elliptic Curve DH and MQC [SP80056A]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
RSA [SP80056B]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035

Santander

Augmented Mosca's theorem



Organizations (CROs, CCOs) need to frame quantum safety as an **Emerging Risk**

Santander

Active regulations

EU DORA

Section 4

Encryption and cryptography

Article 6

Encryption and cryptographic controls

1. As part of their ICT security policies, procedures, protocols, and tools referred to in Article 9(2) of Regulation (EU) 2022/2554, financial entities shall develop, document, and implement a policy on encryption and cryptographic controls.

2. Financial entities shall design the policy on encryption and cryptographic controls referred to in paragraph 1 on the basis of the results of an approved data classification and ICT risk assessment. That policy shall contain rules for all of the following:

(a) the encryption of data at rest and in transit;

(b) the encryption of data in use, where necessary;

(c) the encryption of internal network connections and traffic with external parties;

(d) the cryptographic key management referred to in Article 7, laying down rules on the correct use, protection, and lifecycle of cryptographic keys.

For the purposes of point (b), where encryption of data in use is not possible, financial entities shall process data in use in a separated and protected environment, or take equivalent measures to ensure the confidentiality, integrity, authenticity, and availability of data.

3. Financial entities shall include in the policy on encryption and cryptographic controls referred to in paragraph 1 criteria for the selection of cryptographic techniques and use practices, taking into account leading practices, and standards as defined in Article 2, point (1), of Regulation (EU) No 1025/2012, and the classification of relevant ICT assets established in accordance with Article 8(1) of Regulation (EU) 2022/2554. Financial entities that are not able to adhere to the leading practices or standards, or to use the most reliable techniques, shall adopt mitigation and monitoring measures that ensure resilience against cyber threats.

4. Financial entities shall include in the policy on encryption and cryptographic controls referred to in paragraph 1

PCI DSS

PCI Security Standards Council

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Protocols and encryption strengths may quickly change or be deprecated due to identification of vulnerabilities or design flaws. In order to support current and future data security needs, entities need to know where cryptography is used and understand how they would be able to respond rapidly to changes impacting the strength of their cryptographic implementations. **Good Practice** Cryptographic agility is important to ensure an alternative to the original encryption method or cryptographic primitive is available, with plans to upgrade to the alternative without significant change to system infrastructure. For example, if the entity is aware of when protocols or algorithms will be deprecated by standards bodies, it can make proactive plans to upgrade before the deprecation is impactful to operations. **Definitions** "Cryptographic agility" refers to the ability to monitor and manage the encryption and related verification technologies deployed across an organization. **Further Information** Refer to *NIST SP 800-131a, Transitioning the Use of Cryptographic Algorithms and Key Lengths.*
12.3.3 Cryptographic cipher suites and protocols in use are documented and reviewed at least once every 12 months, including at least the following: • An up-to-date inventory of all cryptographic cipher suites and protocols in use, including purpose and where used. • Active monitoring of industry trends regarding continued viability of all cryptographic cipher suites and protocols in use. • A documented strategy to respond to anticipated changes in cryptographic vulnerabilities.	**12.3.3** Examine documentation for cryptographic suites and protocols in use and interview personnel to verify the documentation and review is in accordance with all elements specified in this requirement.	
Customized Approach Objective		
The entity is able to respond quickly to any vulnerabilities in cryptographic protocols or algorithms, where those vulnerabilities affect protection of cardholder data.		
Applicability Notes		
The requirement applies to all cryptographic suites and protocols used to meet PCI DSS requirements. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

Payment Card Industry Data Security Standard: Requirements and Testing Procedures, v4.0 *March 2022*
© 2006 - 2022 PCI Security Standards Council, LLC. All rights reserved. *Page 267*

In force after: **January 17th, 2025**

April 1st, 2025

Financial entities should follow a flexible approach, based on risk mitigation and monitoring, to deal with the dynamic landscape of cryptographic threats, including threats from quantum advancements.

DORA, RTS for ICT Risk Management (Whereas 9)

Santander

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401774
https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf

MAS recommendation

Monetary Authority of Singapore

10 Shenton Way MAS Building Singapore 079117
Telephone: (65) 6225-5577

Circular No. MAS/TCRS/2024/01

20 February 2024

To Chief Executive Officers of All Financial Institutions

Dear Sir / Madam

ADVISORY ON ADDRESSING THE CYBERSECURITY RISKS ASSOCIATED WITH QUANTUM

Quantum computers that harness the laws of quantum mechanics have the potential to solve certain mathematical problems exponentially faster than traditional computers to bring substantive transformation to a diverse range of industries. At the same time, their potential to break some of the commonly used encryption and digital signature algorithms poses a major cybersecurity concern. The security of financial transactions and sensitive data that financial institutions ("FIs") process could be at risk with the advent of these cryptographically relevant quantum computers ("CRQCs")[1].

2 Leading experts forecast that cybersecurity risks associated with quantum will materialize in the coming decade[2,3]. CRQCs would break commonly-used asymmetric cryptography, while symmetric cryptography could require larger key sizes to remain secure. To that end, NIST has started a global standardisation process for post-quantum cryptography ("PQC"). This involves shortlisting quantum-resistant public-key cryptographic algorithms which would have the capability to operate with existing networking and communication protocols, and protect sensitive information against CRQCs[4]. At the same time, research initiatives involving Quantum Key Distribution ("QKD") technology to establish secure communication channels for distributing encryption keys are in progress[5].

3 To address the cybersecurity risks associated with quantum, FIs need to attain crypto-agility to be able to efficiently migrate away from the vulnerable cryptographic algorithms to PQC without significantly impacting their information technology (IT) systems and infrastructure. FIs could also implement other quantum security solutions, such as QKD, as

[1] CRQC refers to a quantum computer that can efficiently break real world cryptographic systems.
[2] World Economic Forum. (2022). Transitioning to a Quantum-Secure Economy (pp. 9).
[3] NIST. (2016). Report on Post-Quantum Cryptography (pp.6).
[4] NIST announced the first four quantum resistant algorithms in July 2022 that would become part of the post-quantum cryptographic ("PQC") standard. The chosen algorithms are CRYSTALS-Kyber for public key encryption to access secure websites, and CRYSTALS-Dilithium, FALCON, and SPHINCS+ for digital signature.
[5] World Economic Forum. (2022). Transitioning to a Quantum-Secure Economy (pp. 24).

👉 Monetary Authority of Singapore explains in a circular to FI CEOs on Feb 20th, 2024, the need to attain crypto-agility to be able to efficiently migrate away from the vulnerable cryptographic algorithms to PQC without significantly impacting their information technology systems and infrastructure.

The key recommendations in the letter are:

📌 Keeping abreast of the latest developments in quantum computing, and **raising awareness** of the associated cybersecurity risks

📌 **Maintaining an inventory** of cryptographic assets, and identifying critical assets to be prioritised for migration to quantum-resistant encryption and key distribution

📌 Developing strategies and **building capabilities** to address cybersecurity risks associated with quantum

https://www.mas.gov.sg/regulation/circulars/advisory-on-addressing-the-cybersecurity-risks-associated-with-quantum

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

परिपत्र / CIRCULAR

SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113 *August 20, 2024*

प्रति	To,
सभी आनुकल्पिक निवेश निधियाँ (एआईफ)	All Alternative Investment Funds (AIFs)
सभी निर्गमन बैंकर और स्व-प्रमाणित सिंडीकेट बैंक	All Bankers to an Issue (BTI) and Self-Certified Syndicate Banks (SCSBs)
सभी समाशोधन निगम (क्लीयरिंग कारपोरेशन)	All Clearing Corporations
सभी सामूहिक निवेश स्कीमें	All Collective Investment Schemes (CIS)
सभी क्रेडिट रेटिंग एजेंसियाँ	All Credit Rating Agencies (CRAs)
सभी अभिरक्षक (कस्टोडियन)	All Custodians
सभी डिबेंचर न्यासी (ट्रस्टी)	All Debenture Trustees (DTs)
सभी निक्षेपागार (डिपॉज़िटरी)	All Depositories
सभी अभिहित निक्षेपागार सहभागी (डीडीपी)	All Designated Depository Participants (DDPs)
सभी निक्षेपागार सहभागी (डिपॉज़िटरी पार्टिसिपेंट) [निक्षेपागारों (डिपॉज़िटरी) के जरिए]	All Depository Participants through Depositories
सभी निवेश सलाहकार / अनुसंधान विश्लेषक	All Investment Advisors (IAs) / Research Analysts (RAs)
सभी केवाईसी रजिस्ट्रीकरण एजेंसियाँ	All KYC Registration Agencies (KRAs)
सभी मर्चेंट बैंकर	All Merchant Bankers (MBs)
सभी म्यूचुअल फंड / असेट मैनेजमेंट कंपनियाँ	All Mutual Funds (MFs)/ Asset Management Companies (AMCs)
सभी पोर्टफोलियो प्रबंधक	All Portfolio Managers
सभी निर्गम रजिस्ट्रार और शेयर अंतरण अभिकर्ता (आरटीए)	All Registrar to an Issue and Share Transfer Agents (RTAs)
सभी स्टॉक दलाल (ब्रोकर) [एक्सचेंजों के जरिए]	All Stock Brokers through Exchanges
सभी स्टॉक एक्सचेंज	All Stock Exchanges
सभी जोखिम पूँजी निधियाँ	All Venture Capital Funds (VCFs)

India Cybersecurity and Cyber Resilience Framework (CSCRF)

Cyber Resilience Goal: Anticipate | Cybersecurity function: Identify

👉 **Risk assessment** (including post-quantum risks) shall be done on a **periodic basis**. Risk assessment shall include comprehensive scenario-based testing for assessing risks.

Indicative measures to mitigate these risks:

📌 Maintain an inventory of cryptographic assets, prioritizing critical assets for PQC migration, and assess their IT infrastructure capabilities.

📌 Develop strategies for the protection of assets which can and cannot be migrated to PQC.

📌 Upgrade employees' skills, periodically revise policies and conduct proof-of-concept trials.

📌 Explore the feasibility to adopt PQC and technologies like Quantum Key Distribution (QKD).

📌 Monitor ongoing quantum computing developments for cybersecurity threats and ensure that senior management and relevant third-party service providers are aware of the possible risks associated with this technology.

📌 Enhance their crypto-agility.

👉 Prioritization for PQC migration should be based on **the risk assessment**, **criticality** of the asset, **sensitivity** of the information it protects, and its **exposure** to potential threats.

Comply by April 01, 2025

https://www.sebi.gov.in/sebi_data/faqfiles/jun-2025/1749647139924.pdf

https://www.sebi.gov.in/legal/circulars/aug-2024/cybersecurity-and-cyber-resilience-framework-cscrf-for-sebi-regulated-entities-res-_85964.html

January 7, 2025

To: Banking Corporations and Licensed Payment Service Providers
Chairman of the Board and CEO

Subject: **Banking System Preparedness for Cyber Risks Arising from Quantum Computing Capabilities**

Quantum Computing

1. Quantum computing is an innovative technology with the potential to solve complex mathematical problems that were previously unsolvable with existing computing capabilities. This technology is expected to bring significant changes across a wide range of fields and industries.
2. However, alongside the advantages of this development, a sufficiently powerful quantum computer could break widely-used asymmetric encryption algorithms and weaken other encryptions (hereinafter: encryption breaking in the quantum computing era). These encryption methods form the basis for digital signatures and encrypted communication over the Internet. As a result, the security and confidentiality of financial transactions and sensitive data processed by financial institutions could be at risk with the advent of sufficiently powerful quantum computers. The risk involves the exposure of encrypted information and the compromise of the integrity of signatures and signed information.
3. Until recently, experts and analysts in the field of information systems estimated that the feasibility of a quantum computer with the required power was decades away. However, since 2022, due to advancements in building stronger and more stable quantum computers, timelines have shortened. Currently, leading professionals, including analysts and international bodies[1], estimate that the risks of encryption breaking in the quantum computing era will materialize within the next decade, or even sooner.
4. The American National Institute of Standards and Technology (NIST) has initiated a global standardization process for post-quantum cryptography (PQC). This process includes selecting cryptographic algorithms that can operate with existing network and communication protocols and protect sensitive information from encryption breaking in the quantum computing era. Simultaneously, research initiatives are being tested, including quantum key distribution (QKD) technology for establishing secure communication channels for encryption key distribution.
5. The most immediate risk associated with encryption breaking in the quantum computing era is the potential for valuable long-term data, where encryption is of essential, to be quickly deciphered once encryption-breaking capabilities are available. This risk, known as "Harvest Now, Decrypt Later," refers to the possibility of stealing encrypted information collected in various cyber events now and storing it until it can be easily decrypted.

[1] World Economic Forum - WEF (2022). "Transitioning to a Quantum-Secure Economy" (p. 9);
Monetary Authority of Singapore - MAS (2024). "Advisory on Addressing the Cybersecurity Risks Associated with Quantum";
National Institute of Standards and Technology - NIST (2016). "Report on Post Quantum Cryptography (p. 6).

Bank of Israel requirement

👉 It is important to prepare the banking system for information security and cyber risks related to quantum computing.

👉 Organizations are required, at a minimum, to:

📌 Raise awareness within the banking corporation, continuously monitor developments in quantum computing, and assess the associated cyber risks

Inform all relevant parties within the banking corporation, including the board of directors and senior management

📌 Mapping and Managing Encrypted Information Assets

📌 Development of skills and capabilities

Organizations are required to develop an initial plan addressing these points. The plan should be discussed by the board of directors and management.

📅 This preparedness plan should be submitted to the Banking Supervision Department within one year from the date of the directive (January 7th, 2025).

https://boi.org.il/en/economic-roles/supervision-and-regulation/letters/letter202501en/

Image generated with Bing

Results of the issues:

Lack of strategic programs

The need for global coordination

FS-ISAC

QSFF QUANTUM SAFE FINANCIAL FORUM

QRWGCFDIR Quantum-Readiness Working Group of the Canadian Forum for Digital Infrastructure Resilience

The Timeline for Post Quantum Cryptographic Migration

A Position Paper on the Financial Sector's Global Transition

Produced in collaboration by the FS-ISAC Post Quantum Cryptography Working Group, members of the Quantum-Readiness Working Group (QRWG) of the Canadian Forum for Digital Infrastructure Resilience (CFDIR), and the Quantum Safe Financial Forum

TLP WHITE

Given the financial sector's extensive interconnectivity, a synchronized migration strategy would streamline the transition by addressing key bottlenecks, including the following.

Fragmentation

Misaligned strategies due to the adoption of incompatible approaches or divergent timelines among firms.

Confusion

Misaligned timelines across multiple jurisdictions, creating conflicts, uncertainty, and difficulty in executing migration.

Prolonged reliance on outdated cryptography

Quantum-vulnerable cryptography deprecation delayed by the need to maintain backward compatibility with slow movers.

Duplicated effort

Wasted resources as firms independently solve the same challenges without sharing knowledge.

https://www.fsisac.com/the-timeline-for-post-quantum-cryptographic-migration

Positive impact of timelines

FS-ISAC QSFF QRWGCFDIR

The Timeline for Post Quantum Cryptographic Migration

A Position Paper on the Financial Sector's Global Transition

Produced in collaboration by the FS-ISAC Post Quantum Cryptography Working Group, members of the Quantum-Readiness Working Group (QRWG) of the Canadian Forum for Digital Infrastructure Resilience (CFDIR), and the Quantum Safe Financial Forum

TLP WHITE

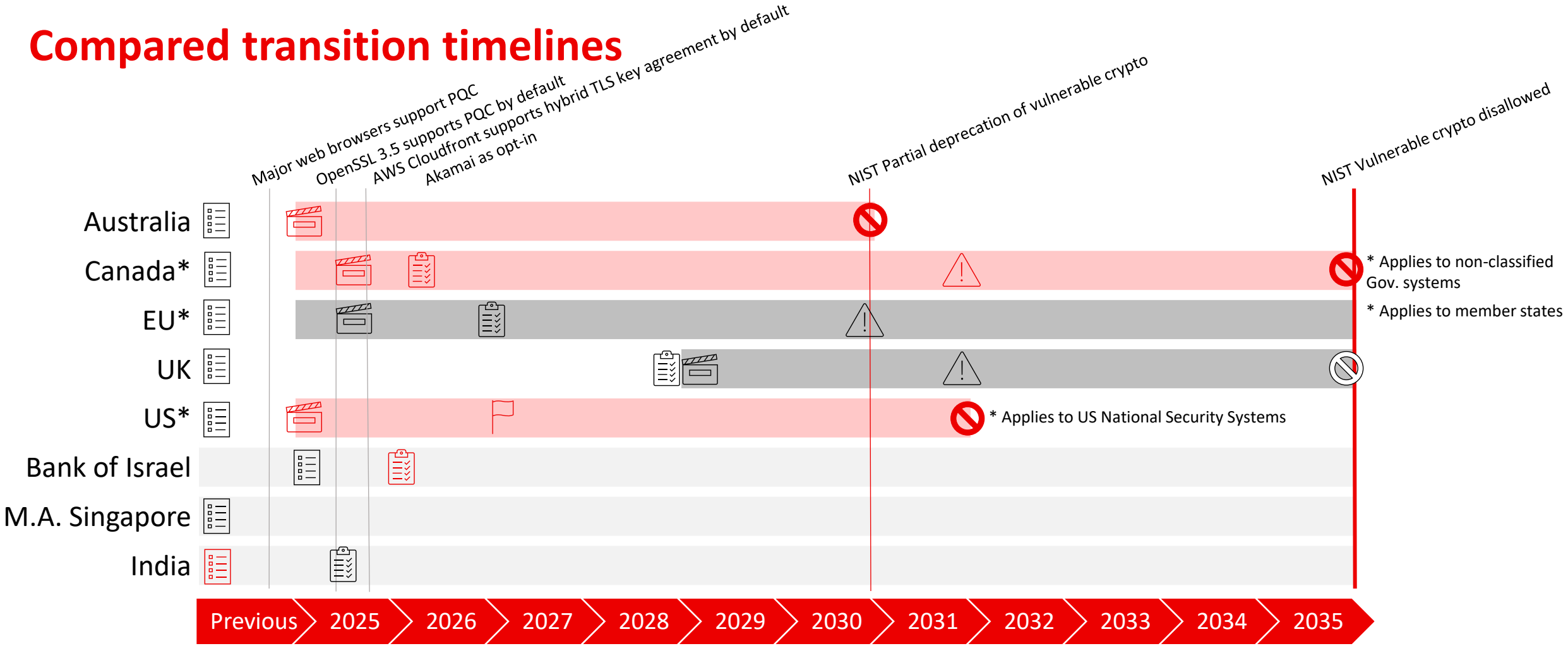
The positive impact of influential timelines was demonstrated by the first version of the US National Security Agency's (NSA) transition plan, Commercial National Security Algorithm Suite 2.0 (CNSA 2.0), published in 2022.[v]

By publishing its internal transition timeline, the US government and its NSA achieved three key goals:

1. Provided public visibility of their roadmap.
2. Established milestones for national security system administrators.
3. Informed its vendors and service providers of what the US government will expect from them.

https://www.fsisac.com/the-timeline-for-post-quantum-cryptographic-migration

Compared transition timelines



Category

- Recommendations and guidelines
- Policies and requirements
- Clearly specified timelines
- Financial sector specific

Planning Activities

- Start planning
- Complete planning

PQC Implementation Activities

- Start implementing PQC
- New deployments must use PQC
- Complete the migration on most sensible use cases
- Stop using vulnerable cryptography

Santander

FS-ISAC QSFF QRWGCFDIR

The Timeline for Post Quantum Cryptographic Migration

A Position Paper on the Financial Sector's Global Transition

Produced in collaboration by the FS-ISAC Post Quantum Cryptography Working Group, members of the Quantum-Readiness Working Group (QRWG) of the Canadian Forum for Digital Infrastructure Resilience (CFDIR), and the Quantum Safe Financial Forum

TLP WHITE

Summary

Situation

- Consensus is limited around the target dates

Proposes

- Guidance from authoritative agencies would:
  - Inform a coordinated global transition timeline
  - Generate a top-down approach in financial institutions

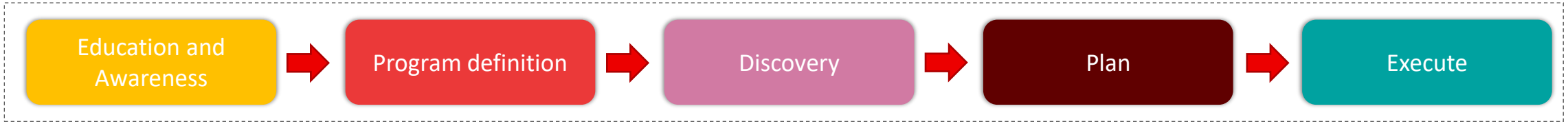
- The guidance should convene clear and reasonable milestones that:
  - Enforce action.
  - Facilitate compliance with local policies and regulations across jurisdictions.
  - Reduce the need to maintain backward compatibility.

Reminds

- Post quantum cryptographic resilience is not a competition, but a collaborative project.

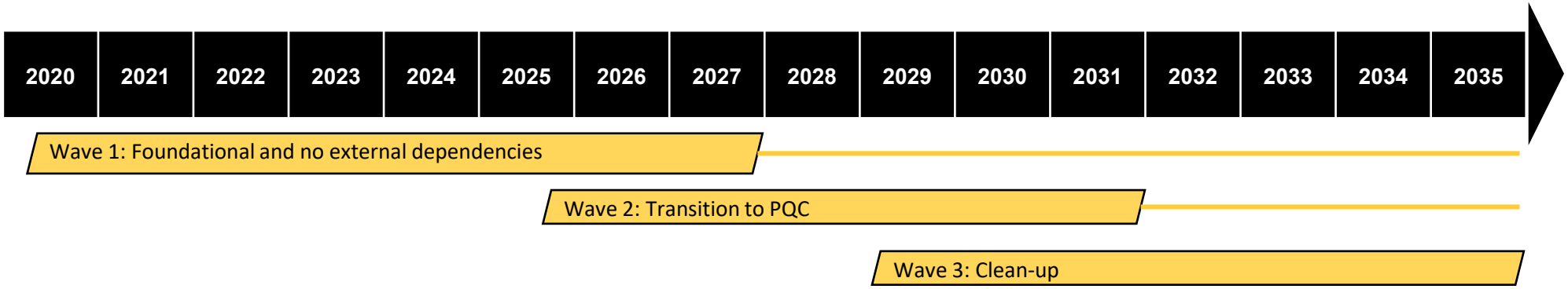
https://www.fsisac.com/the-timeline-for-post-quantum-cryptographic-migration

Roadmap to Quantum-Readiness



Santander's **long-term timeline** considers three main waves:

- **Wave 1 Foundational activities and those without external dependencies** (No-Regret Actions)
- **Wave 2 Transition to PQC**
- **Wave 3 Clean-up**

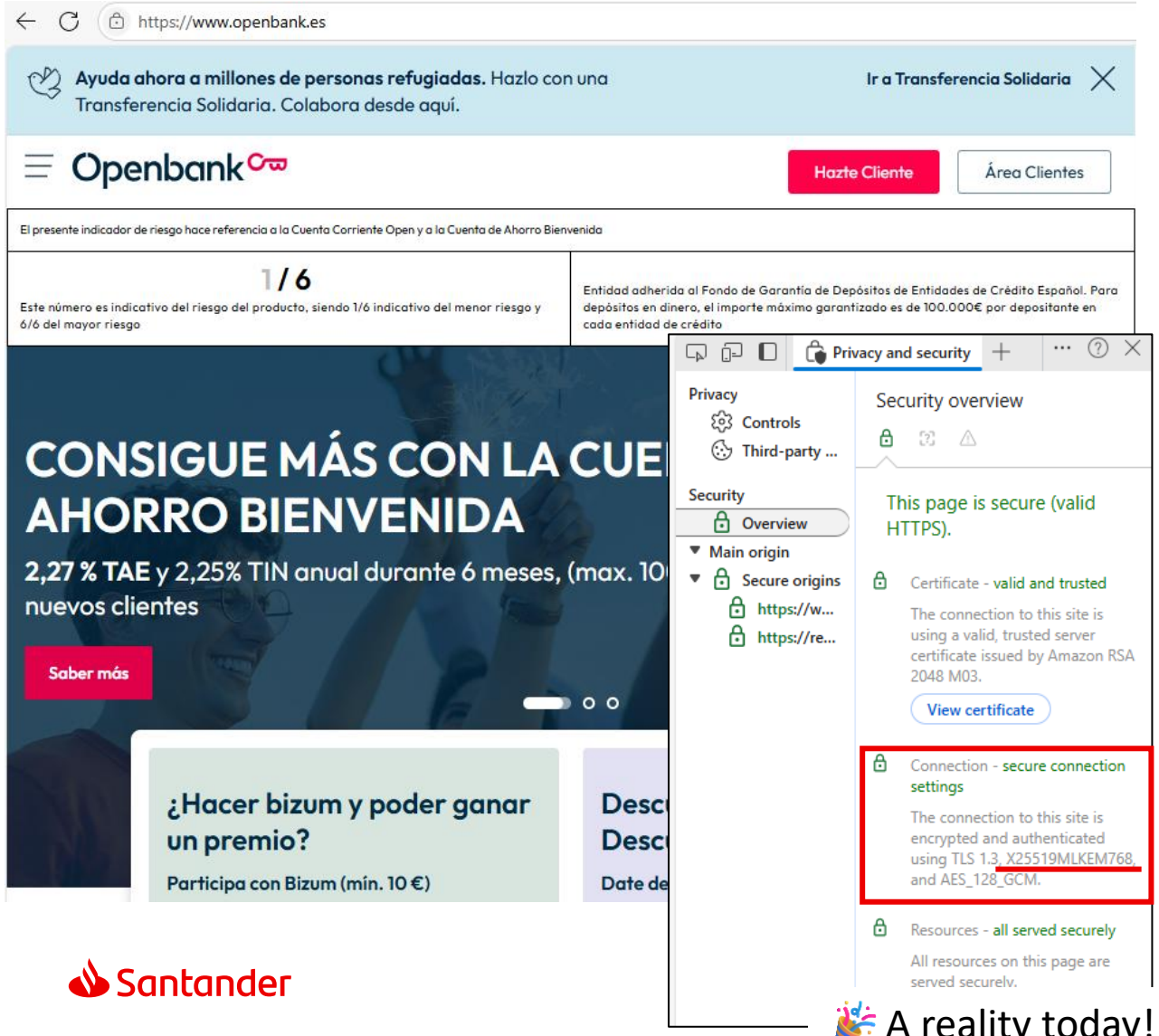


Sector-wide timelines should guide the following **milestones**, per each **use case**:

- **PQC Introduction** When to initiate deployment of PQC -> Identify dependencies and their roadmaps
- **Sunset start for classical cryptography** When to stop supporting classical cryptography in new projects
- **End of backward compatibility** When to stop supporting classical cryptography in any project

Specific use cases where banks can act now

Confidentiality protection in transactional websites: **An easy first goal**



Protection	Confidentiality
Actionability	**High** – Most CDNs will support PQC by 1Q2026
Intricacy	**Low** – Most browsers support PQC since 2024. Standard solutions available for the bank and client side
Action	Start testing implementation

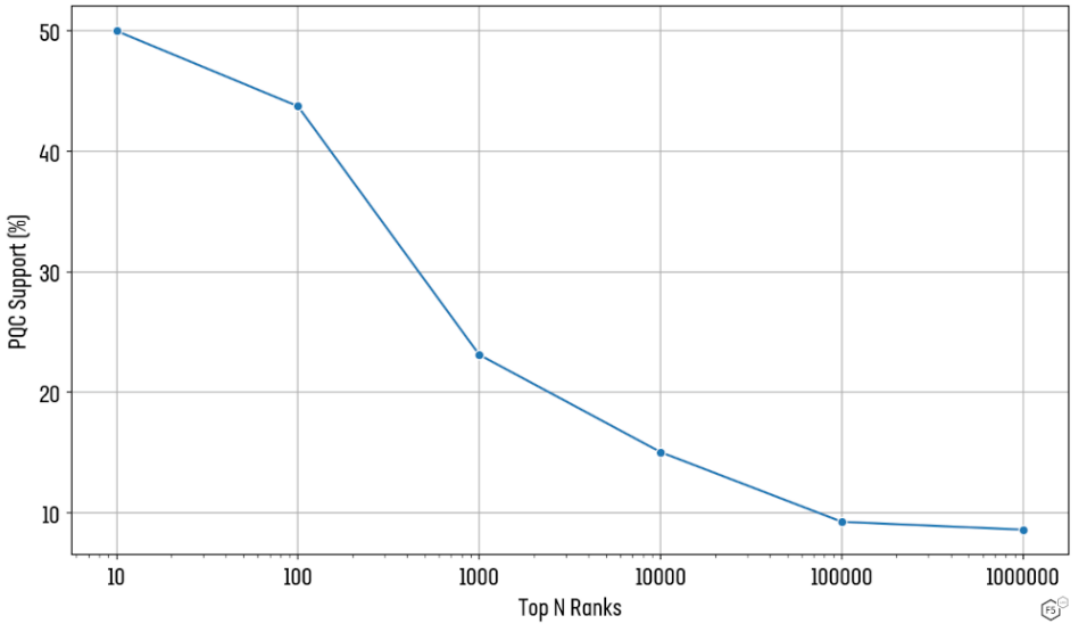


Figure 3: Percentage of sites across the top 1M which support PQC (logarithmic scale)

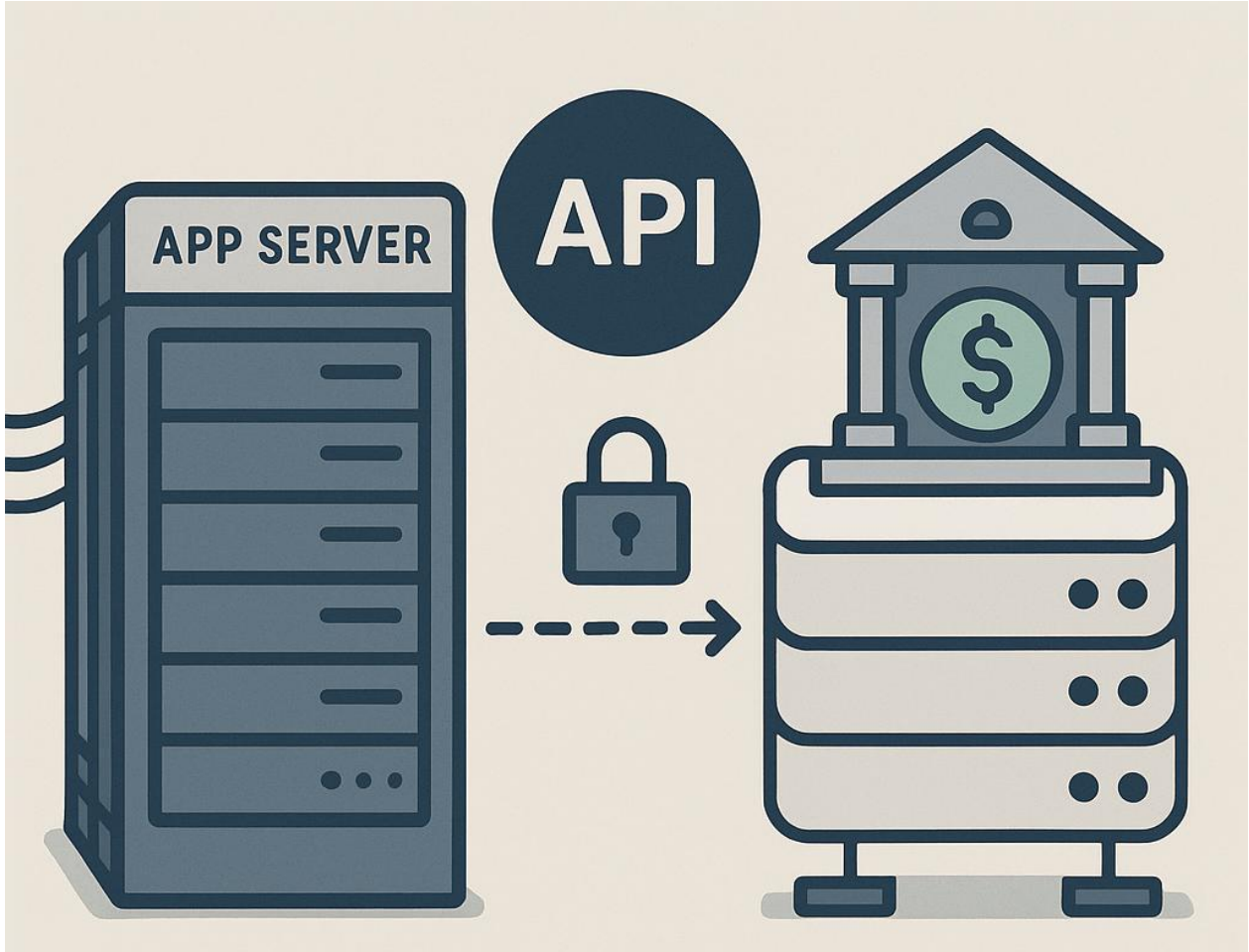
Santander

🎉 A reality today!

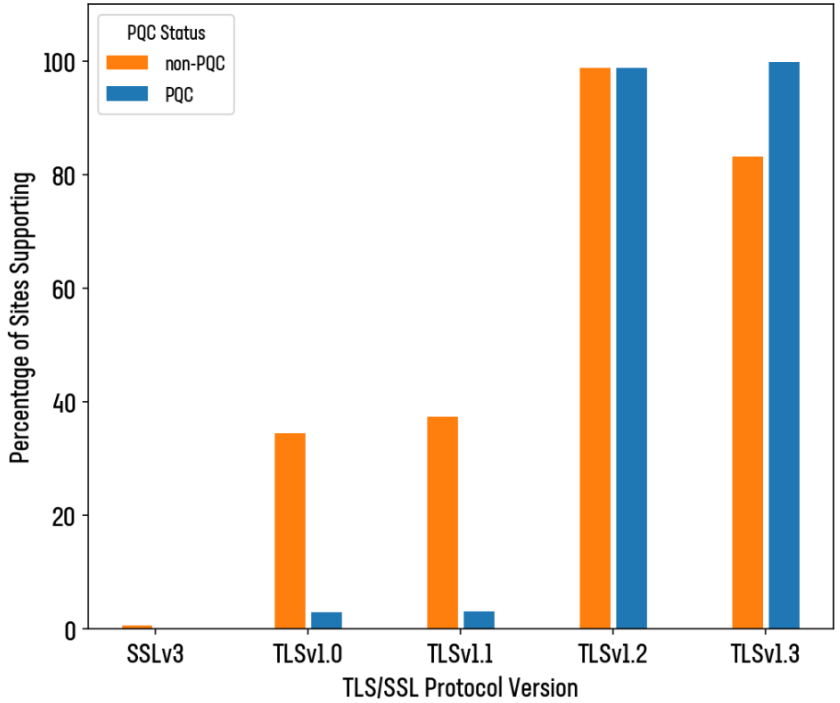
https://www.f5.com/labs/articles/threat-intelligence/the-state-of-pqc-on-the-web , June 2025

Specific use cases where banks can act now

Confidentiality protection in API services: Start tackling future **backward compatibility challenges**



Protection	Confidentiality
Actionability	**High** – Most CDNs will support PQC by 1Q2026. TLS negotiation monitoring is relatively simple.
Intricacy	**Medium** – API clients are not updated often, hence their support for PQC will be limited.
Action	Monitor TLS negotiation to understand who and why depending on obsolete parameters. Start planning to decommission insecure configurations.



https://www.f5.com/labs/articles/threat-intelligence/the-state-of-pqc-on-the-web , June 2025

Specific use cases where banks can act now

Confidentiality protection in secure file transfers: An opportunity to agree on **common protection standards**

Protection	Confidentiality
Actionability	Medium – Although foundational software and libraries already support PQC by default, their deployment in enterprise Operating Systems and products is still limited.
Intricacy	Medium – The adoption of PQC will depend on peer-to-peer negotiations. Establishing a sector-wide plan would streamline the transition
Action	Collaborate within the sector to agree on a transition roadmap and parameters

Specific use cases where banks can act now

Long-term protection of digital signatures in contracts: Plan the second stage and **minimize future mitigation projects**

Protection	Signatures
Actionability	Medium – Solutions to implement PQ digital signatures exist, but PQC certificates still need some time
Intricacy	Medium – PDF readers do not support PQC signatures yet
Action	Plan how to introduce PQC signatures in your legal documents, expecting current technical dependencies to be solved around 2027 (possibly)

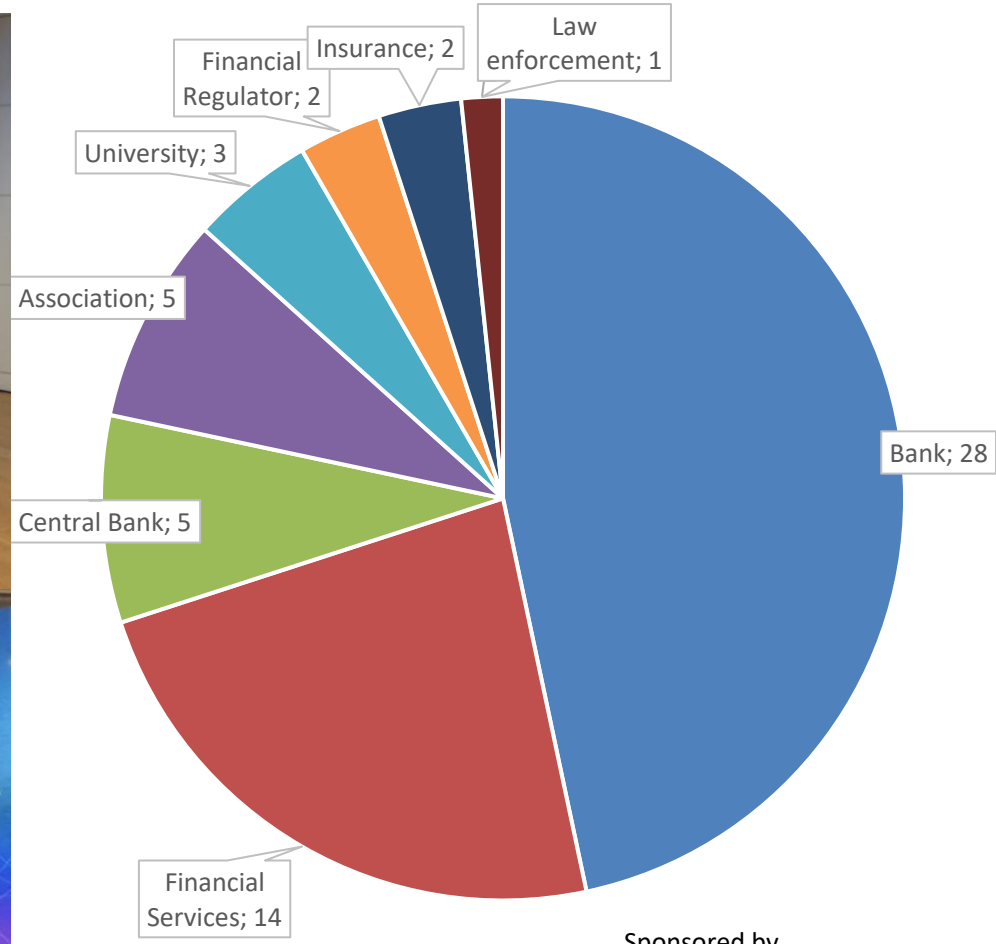
Specific use cases where banks can act now

PQC support in Point of Sale terminals: Design now the **roadmap of long-term, intricate projects**

Protection	Authentication
Actionability	**Low** – Solutions are not available yet
Intricacy	**High** – The transition may require complex software or hardware upgrades at scale. It may need to be coordinated with the terminals' deprecation lifecycle
Action	Promote vendor/industry collaboration to test and agree on a transition roadmap

Europol Quantum Safe Financial Forum

Quantum Safe Financial Forum members
(Total as of Oct. 9th 2025, 60 members)



Sponsored by

Santander

QSFF QUANTUM SAFE FINANCIAL FORUM

EUROPOL

https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/qsff


START
00:00:00
PQC MARATHON
PQC MARATHON
PQC MARATHON


PQC MARATHON
FINISH
PQC MARATHON
PQC MARATHON
04:15:37
PQC MARATHON
PQC MARATHON

Thank You.

Our purpose is to help people and businesses prosper.

Our culture is based on believing that everything we do should be:

Simple Personal Fair

Santander