

Post-Quantum Crypto Transition for Global Financial Institutions

Disclaimer

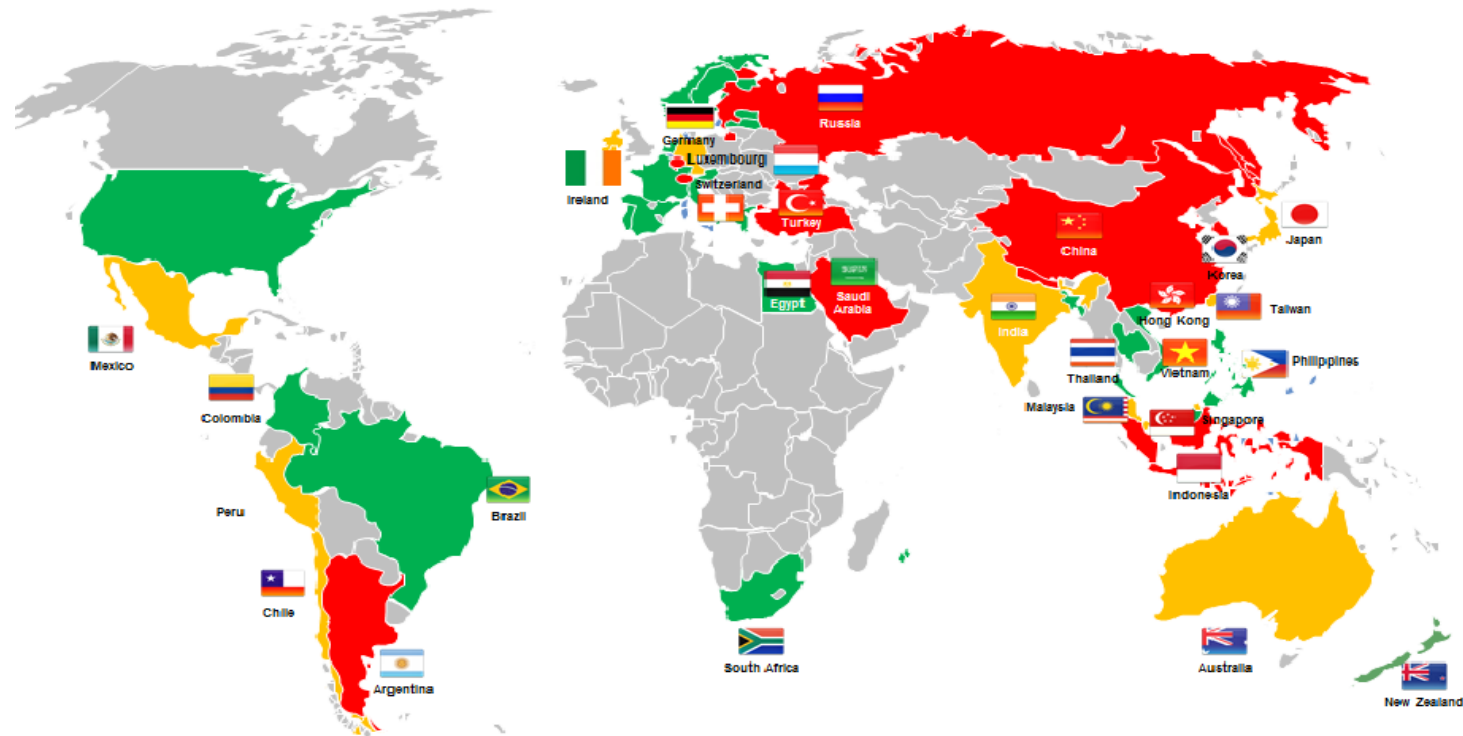
2020 JPMorgan Chase & Co. All rights reserved. Chase, JPMorgan and JPMorgan Chase are marketing names for certain businesses of JPMorgan Chase & Co. and its subsidiaries worldwide (collectively, “JPMC”). Products and services may be provided by commercial bank affiliates, securities affiliates or other JPMC affiliates or entities. Not all products and services are available in all geographic areas. Eligibility for particular products and services is subject to final determination by JPMC and or its affiliates/subsidiaries.

This material is provided to you for informational purposes only; and any use for other than informational purposes is disclaimed. It is a summary and does not purport to set forth all applicable terms or issues. It is not intended as an offer or solicitation for the purchase or sale of any financial product and is not a commitment by JPMC as to the availability of any such product at any time. The information herein is not intended to constitute legal, tax, or accounting advice and you should consult your own advisors as to such matters and the suitability of any transaction. JPMC makes no representations as to such matters or any other effects of any transaction. In no event shall JPMC be liable for any use of, for any decision made or action taken in reliance upon, or for any inaccuracies or errors in, or omissions from, the information herein.

The material contained herein is intended as a general commentary. Opinions expressed herein are those of Yassir Nawaz and may differ from those of other JPMC employees and affiliates. This information in no way constitutes JPMC research and should not be treated as such. Further, the views expressed herein may differ from that contained in JPMC research reports. The statistics quoted herein have been obtained from sources deemed to be reliable, but we do not guarantee their accuracy or completeness.

Global Financial Institutions Are Highly Regulated

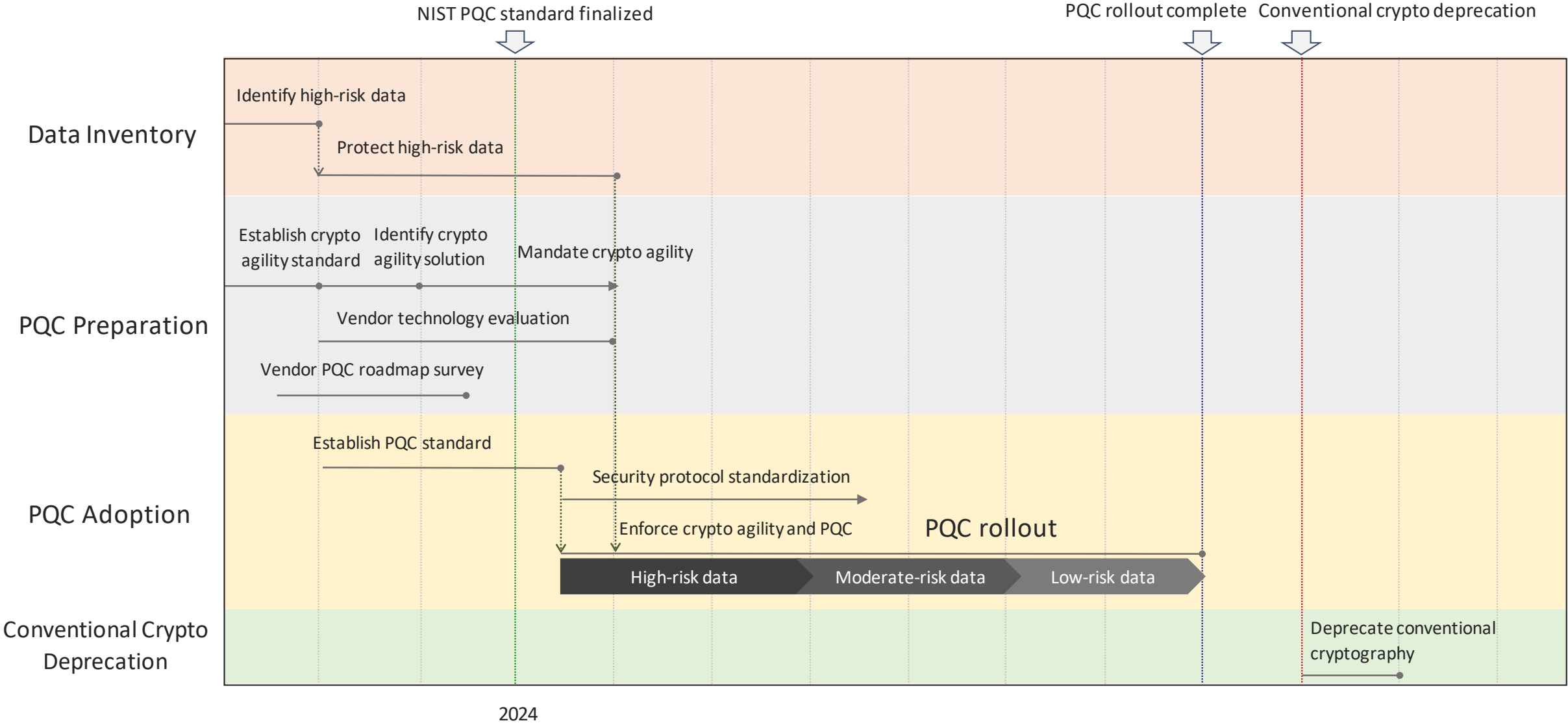
- 60+ regulators engage with JPMC on Cybersecurity – all with their own standards, frameworks and requirements.
- JPMC needs to support myriad of crypto and key management standards.



Considerations for Post-Quantum Cryptography Transition

- Replacing major components of cryptographic infrastructure is complicated and time-consuming, since these systems need to demonstrate the highest level of trustworthiness, reliability and interoperability.
- Considerations for financial institutions
 - 1) Data-centric and risk-based approach to PQC transition
 - 2) Uplift crypto policy for post-quantum cryptography
 - 3) Drive PQC transition through adoption of crypto agility – require system to be certified for crypto agility before PQC
 - 4) Participate in security protocol standardization to reflect financial industry's interests and institution's priorities
- Organizations that choose the crypto agility path will realize there is a lack of authoritative related standard or guidance.

Reference PQC Transition Timeline



Challenges with Crypto Agility

Crypto Agility Requirements	
Crypto User (Application)	Crypto Provider (Solution)
1. Cypto User (“Application”) should be agnostic to the algorithm (e.g., AES) and configuration (e.g., key length) used in performing crypto operation. 2. Application should perform cryptographic operation without having to access raw keying material (e.g. master key, data key). 3. Application code refactoring is permitted for integration with another Solution or to take advantage of a new feature. 4. Application Owner should ensure Solution in use is supported throughout the application and its data lifecycle/lifespan.	1. Cryptographic Solution Provider (“Solution”) should provide crypto agnostic API to its client (or Application). 2. Solution should not provide Application with direct access to raw key material (e.g., data key, master key). 3. Solution should be committed to supporting future NIST crypto standards and guidelines, including the post-quantum cryptography standard. 4. Solution should maintain backward compatibility, i.e., a newer Solution version should be able to process ciphertext generated from an older version. 5. Interoperability with other Solutions is optional, but Solution should provide utilities or APIs to convert its ciphertext to another Solution’s.

Thank you!

Yassir Nawaz

JPMorgan Chase & Co.