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).

part of their risk mitigation. This advisory highlights some of the measures that FIs should consider as part of their quantum transition efforts:

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

a) Monitoring ongoing quantum computing developments for cybersecurity threats and risks that may impact financial services, and their possible mitigation using quantum security solutions such as PQC and QKD.

b) Ensuring that the senior management and relevant third-party vendors understand the potential threats of quantum technology, and the importance of supporting efforts on transitioning to quantum security solutions.

c) Working closely with third-party IT vendors to assess the FI's IT supply chain risks arising from the quantum threats, and requesting that vendors provide quantum-resistant solutions when they become commercially available.

d) Connecting with relevant industry groups, research bodies, or Information Sharing and Analysis Centres ("ISACs") to exchange information and collectively mitigate systemic quantum risks.

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

e) Identifying and maintaining an inventory of cryptographic solutions used in the FI, and determining those which are potentially vulnerable and need to be replaced with quantum-resistant alternatives when the solutions become commercially available. This inventory should include information about:
   i. the cryptographic algorithm and key length used,
   ii. the ownership and parties responsible for maintaining cryptographic assets, and
   iii. the specific system or application where the cryptographic algorithm is embedded or used.

f) Classifying IT and data assets that are dependent on the potentially vulnerable cryptographic solutions, so as to prioritise the risk mitigation efforts. The classification

should be based on the sensitivity, criticality, and risk exposure of the IT and data assets, and the period for which they are deemed sensitive.

g) Assessing whether existing system infrastructures can support crypto-agility, and consider upgrading them over time if there are limitations (e.g. on processing power, infrastructure design, discontinuation of vendor support, etc.) that may hinder the transition to quantum security solutions.

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

h) Uplifting the technical competencies of relevant staff to equip them with the requisite skillsets for supporting the transition to quantum security solutions.

i) Reviewing the FI's internal policies, standards, and procedures, to ensure that they remain relevant as the FI transitions to quantum security solutions.

j) Developing risk mitigation strategies for assets which cannot be migrated to PQC, and planning for contingency scenarios where cybersecurity risks associated with quantum materialize substantially ahead of the predicted timeline.

k) Where resource permits, consider proof-of-concept trials with quantum security solutions to sensitize the FI on their potential impact to operations and implementation challenges. Early experimentation would help the FI to make informed decisions on solutions that become commercially available as the nascent market matures.

4 This advisory should be read as supplementary information to the MAS notices and guidelines[6].

[6]The MAS notices and guidelines include the Notice on Technology Risk Management (TRM), Notice on Cyber Hygiene, TRM Guidelines, and Outsourcing Guidelines.