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).

Prepare the Banking System for the Quantum Computing Era

Given the above, it is important to prepare the banking system for information security and cyber risks related to quantum computing, particularly encryption breaking risks in the quantum computing era, in line with developments in this field. According to Proper Conduct of Banking Business Directive 364 "Management of Information Technology Risks, Information Security, and Cyber Defense" (hereinafter "**Directive 364**") and relevant directives in the fields of information technology, information security, and cyber defense currently in force, you are required to act, at a minimum, as follows:

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

   Establish and implement mechanisms for continuous and ongoing updates on quantum computing developments, increasing knowledge and awareness of relevant information security and cyber risks among all relevant parties within the banking corporation:

   6.1 Inform all relevant parties within the banking corporation, including the board of directors and senior management, to ensure recognition of the potential threats of quantum computing technology and the importance of their support in transitioning to post-quantum security solutions. This topic should be discussed periodically in line with technological developments, at least once every two years, and include a review of general developments in quantum computing, particularly those affecting the banking sector, and the organizational preparedness status for addressing quantum computing risks.

   6.2 Continuously monitor ongoing developments in quantum computing that may impact cyber defense and information security aspects of financial services and the possibility of mitigating them through developments in quantum security solutions such as PQC and QKD, including engaging with relevant industry bodies, research institutions, or knowledge-sharing centers.

   6.3 Integrate quantum computing considerations into the cyber risk management process with the supply chain, maintaining regular contact with third parties to assess the impact of quantum computing developments on the banking corporation's supply chain risks, and requiring relevant third parties to adopt resilient solutions when they become commercially available. Pay special attention to relationships with material software and hardware suppliers and avoid reliance on suppliers and manufacturers that are not preparing for the quantum era or that may pose a technological risk in this era.

7. **Mapping and Managing Encrypted Information Assets**

   Map encrypted information assets.[2] This mapping will enable the banking corporation to understand its exposure to information security and cyber risks relevant to the quantum computing era, and create a transition plan to encryption solutions adapted to the quantum computing era when they become available. The mapping should include:

   7.1 Mapping encrypted information assets at rest, considering the following characteristics:

---

[2] It should be noted that such mapping is part of the process of identifying and classifying activities, processes, and information assets required under Proper Conduct of Banking Business Directive 364 on "Management of Information Technology Risks, Information Security, and Cyber Defense."

i. Type of encryption algorithm and key length.
ii. Information owner's details.
iii. Systems and applications using the algorithm.
iv. Duration for which the encrypted information is valid and must remain encrypted, particularly considering the "Harvest Now, Decrypt Later" risk.
v. Sensitivity and criticality level of the information (personal, medical, national security, business-confidentiality, etc.).

7.2 Mapping processes and systems using asymmetric encryption in motion with external entities.

7.3 Mapping asymmetrically encrypted information outside the organization for any reason (e.g., cloud environment used by the organization, intentional transfer, backup, information leaked due to a past cyber event) with the same mapping characteristics defined in Section 7.1.

8. **Readiness for the development of skills and capabilities to address cyber risks related to quantum computing (according to developments in the field).**
Given the assessments regarding the timing of encryption-breaking capabilities in the quantum computing era, as detailed in Section 3 above, start preparing to build an infrastructure that will enable the banking corporation to be adequately prepared, adapted to the development of the issue (both in terms of risk realization and developments in defensive readiness). Additionally, continuously assess the appropriate timing for advancing the required skills, according to developments. This preparation should include, among other things, addressing and assessing the need for action in the following areas:

8.1 Training employees for the transition processes to the required security solutions.

8.2 Defining the resources needed to establish a laboratory and testing environment for the solutions.

8.3 Assessing the existing computing infrastructure and its compatibility with post-quantum encryption (in terms of computing power, manufacturer support, software versions, etc.).

8.4 Preparing for the transition from vulnerable algorithms to new resilient algorithms when they become available, in a way that minimizes the impact on information systems and infrastructures.

8.5 Identifying policy documents and procedures that are expected to be affected, and formulating a plan to update and validate them to ensure their compatibility with the post-quantum era and the transition to quantum security solutions.

8.6 Defining alternative solutions for cases where systems cannot be converted to post-quantum encryption or if the risk materializes earlier than expected.

You are required to develop an initial preparedness plan addressing the issues outlined above. This plan should be discussed by the board of directors and management.

This preparedness plan should be submitted to the Head of the Technology, Innovation, and Cyber Division at the Banking Supervision Department within one year from the date of this letter. The mapping required in Section 7 above should be completed as part of the banking corporation's preparation to meet the requirements of Proper Conduct of Banking Business Directive 364.

Sincerely,

Daniel Hahiashvili, Supervisor of Banks

Cc: Ms. Tal Harel Matityahu – Deputy Supervisor of Banks, Head of Technology, Innovation, and Cyber Division
Ms. Aya Gal-Ed – Head of the Supervisory Cyber Unit
Ms. Liora Navon – Head of Technology in Banking Unit
Chief Technology Officer
Chief Risk Manager
Head of Cyber Defense