Bank of Israel Supervisor of Banks		

Jerusalem, 12 Tammuz 5775
June 29, 2015
15LM2087

To: The Banking Corporations
Attn: Chief Executive Officer

Re: Risk management in a cloud computing environment

1. Background

In recent years, there has been an increasing trend of moving to various forms of cloud computing. These technologies enable the efficient and convenient use of computer resources by sharing these resources and using them on demand. In addition with savings in equipment costs, data center floor, electricity, etc., which contribute to more environmentally friendly green computing.

Alongside the advantages, the use of such technology may expose the banking corporation to significant operational risks related to information security, business continuity, command and control of IT assets, etc. These risks are derived, inter alia, from dependency on specific suppliers or technologies; management, security, command and control tools that have not yet been matured; difficulties in protecting information and in implementing adequate controls; increasing the potential damage in the case of failure, particularly regarding single points of failure; sensitivity of the technology's designated components; difficulty in separating roles, and more. While some of these risks are known, they contain unique aspects in view of the specific characteristics of these technologies and the fact that these technologies are developing and that the information security tools are not necessarily mature.

2. Applicability

The provisions of this letter shall apply in accordance with the applicability provisions set out in Section 2 of Proper Conduct of Banking Business Directive 357 (hereinafter: "the Directive").

3. General

3.1 A banking corporation shall not make use of cloud computing services for core activities and/or core systems.

3.2 A banking corporation shall not store customer information or data on the cloud outside the borders of the State of Israel, unless it has ascertained that the cloud service provider meets the level of protection in accordance with the directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data directive of the European Union.

3.3 Cloud computing constitutes a private instance of outsourcing as defined in Chapter F of the Directive. Therefore, the banking corporation must act in accordance with Proper Conduct of Banking Business Directive number 357, particularly in relation to that stated in Sections 17, 18 and 30 of the Directive.

3.4 We hereby refer the banking corporations to the relevant laws and regulations for the use of cloud computing technologies, including to the Privacy Protection Law and to the Privacy Protection Regulations (Transfer of Information to Information Databases Outside the Borders of the Country), 5761–2001. In addition, we refer to the Registrar of Information Databases Guideline number 2/2011—"Use of Outsourcing Services for the Processing of Personal Information".

3.5 It is recommended that the banking corporation consult, as relevant, external consultants with expertise in reducing the risks inherent in the use of cloud technologies.

4. Corporate governance

4.1 A banking corporation examining the use of cloud computing technologies, must bring the matter for prior discussion by the Board of Directors, before using cloud computing technologies. At this discussion, the risks inherent in cloud computing technologies and the implemented controls and those planned to be implemented to mitigate the risks, are to be presented. The Board of Directors must discuss these risks, decide whether to grant preliminary approval to the process, and instruct the senior management regarding the actions it must take—including according to those specified in this letter. As relevant, the Board of Directors shall instruct management to formulate and present for its approval a policy document for the use of cloud computing technologies.

4.2 Further to that stated in Section 4.1 above, the Board of Directors shall discuss and approve policy for the use of cloud computing technologies. The policy document shall relate to the accountability, responsibility and operations of cloud service management functions, controls and supervision functions, the types and scope of services, approval processes and approval ranks, the responsibility of various parties at the bank for handling legal, maintenance, monitoring, information security, and other aspects. The policy shall provide a response, inter alia, to the requirements of this letter.

4.3 Before any engagement with cloud computer service provider (hereinafter: "cloud service providers" or "the supplier" or "the provider"), a discussion must be held by management and, as relevant, by the Board of Directors.

4.4 The banking corporation's senior management must make sure that any use of cloud computer technologies shall be in accordance with the policy set forth as stated.

5. Risk management

5.1 Before engaging with cloud service providers, the banking corporation must carry out due diligence, including regarding the provider's financial resilience, professional ability and experience in providing similar services. It is expected that such an examination shall be carried out periodically, during the service period.

5.2 A banking corporation shall carry out risk identification and assessment process for any engagement with a cloud service provider. The risk assessment shall be done prior to the engagement, and shall be updated on an on-going basis during the service period, inter alia in accordance with the following changes: technological; business and organizational changes at the banking corporation or at the cloud service provider; and regulatory. The banking corporation must ascertain the existence of appropriate compensatory controls. Even though cloud computing constitutes a private instance of outsourcing, the risk assessment must also include unique risks (technological and other) related to the use of cloud computing. Examples of aspects that must be taken into account are provided in the appendix. Accordingly, the banking corporation shall ensure that it receives the required information from the cloud service provider for the purpose of carrying out the risk assessment, including that required in Section 6.1.1 below.

5.3 The banking corporation shall ensure that it has the ability to monitor information security incidents related to its use of cloud computing systems. If this monitoring is done through tools provided by the provider, the banking corporation shall ensure that the tools meet the accepted standards and enable integration with the bank's current monitoring tools.

5.4 The banking corporation's information must be encrypted when being transferred over communications lines and when being stored in a multi-tenancy system (a system that is not exclusively for the use of the banking corporation). In cases where it is difficult for the banking corporation to encrypt all of the information as stated, it must encrypt at least the information that it classifies as sensitive, that may harm the banking corporation or its customers if being exposed. The encryption keys shall be stored at the banking corporation and not at the provider.

6. Agreement with the cloud service provider

6.1 The service agreement with the provider shall include, among other things, the following requirements:

6.1.1 Receiving from the provider internal and external audit reports conducted on its operations, including audit reports carried out by regulatory entities. In addition, the agreement shall enable the banking corporation to require the provider to carry out, on particular cases, an audit on a specific subject.

6.1.2 The existence of a unilateral possibility that the banking corporation may cease the engagement with the provider or move to a different provider, including transferring its relevant data from the provider's system within a short time, their deletion from the provider's system, and the provider's obligation that it will not be possible to review these data in its system.

6.1.3 Granting the Banking Supervision Department the ability to conduct an audit at the provider's premises.

6.2 In any change in ownership of the cloud service provider, the banking corporation must re-examine the engagement in order to ensure the new ownership's fulfillment of obligations toward the banking corporation.

7. Obtaining a permit from the Supervisor of Banks

Notwithstanding that stated in Section 3.3 above, the banking corporation is required to obtain in advance a written permit from the Supervisor of Banks, prior to any engagement with a cloud service provider, as part of which information is stored with the provider, even if it is not customer information. In order to obtain the permit, the bank must apply to the Banking Supervision Department at least 60 days before using the service.

8. Start date

The provisions of this letter will come into force on the date of its publication.

Sincerely,

David Zaken
Supervisor of Banks

Appendix—Risk assessment – Examples of cloud computing aspects

- Corporate governance, policy and procedures, internal and external audits— Do the policy documents properly relate to the use of cloud computing?
- Regulatory risk—difficulty in adhering to the laws and regulations of the State of Israel and of the state in where the system operates, or the system and/or the data are stored. It is important, inter alia, to take into consideration issues such as the provider's obligation to provide information to law and enforcement entities even without the knowledge of the banking corporation. There are many legal aspects related to the non-uniformity of definitions and the requirements in various countries.
- Systemic risk derived from a cloud service provider who provides services to a number of banking corporations.
- Life cycle of the data, including location, multiplicity of copies and exposure of data.
- Data transferring, components and systems - for instance, does the use of a particular provider's cloud components limit the banking corporation and could prevent it from being able to move to another provider or transfer the information and/or systems back to the bank's premises?
- Information security, including changes in the traditional concept and the use of designated security tools.
- Access controls, while using the appropriate tools for the cloud computing environment.
- Change management and information technology asset management—for instance, does the banking corporation have control over changes in the systems and are the changes in line with the banking corporation's policy and procedures?
- Risks related to business continuity and BCP/DRP, including changes in the banking corporation's network configuration. Management tools and environments that may add a level of complexity and sophistication to the systems.
- Legal risks, including aspects of confidentiality, data maintenance, ownership of information and licensing of software.
- Incident management, including reporting and handling procedures, and responsibilities definition.