Bank of Israel
Banking Supervision Department
Policy and Regulation Division

Tel Aviv, July 5, 2017
Circular no. C-06-2536

Attn:
Banking corporations and credit card companies

Re: Cloud computing
(Proper Conduct of Banking Business Directive no. 362)

General remarks

1. In recent years, organizations in Israel and abroad have been increasing their use of cloud-computing technologies. These technologies allow them to reduce their computing expenses - hardware, infrastructure, software, data center space - and save energy by making the use of computer resources efficient and convenient and the possibility of sharing resources and using them as needed. Cloud computing follows three principal models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The use of cloud-computing technologies may help a banking corporation comply with the TTM (Time to Market) principle. For example, it may speed up systems development process considerably by using the PaaS model or obviate the need for in-house development and use of SaaS software, which was developed, installed, and operated in the cloud.
2. Cloud computing is a form of outsourcing. Notwithstanding its advantages, using cloud technologies may expose a banking corporation to material operational risks and cyber and information-security risks such as leakage of sensitive information, disruption of business continuity, harming the command and control of IT assets, etc. These risks originate, among other factors, in dependency on specific service providers or technologies; weakening of command-and-control of the use of cloud technologies; difficulties in protecting information and applying adequate controls; intensification of potential damage in the event of a failure, particularly when single points of failure occur; sensitivity of dedicated components of the technology; difficulty in Segregation of Duties, etc. Given the specific characteristics of cloud-computing technologies compared to the traditional outsourcing, along with the fact that the control and security tools are not necessarily mature, they pose unique and known risks that, when they materialized, the damage to a banking corporation can be significant and major.
3. This Directive cancels the letter from the Supervisor of Banks on “Risk management in a cloud computing environment”, dated June 29, 2015, in which conditions for the use of cloud-computing technologies by a banking corporation were spelled out for the first time. In the letter, the Supervisor instructed banking corporations to apply to the Banking Supervision Department for a permit before they use any cloud-computing technology. In view of the experience amassed on the topic by both the Supervision Department and the banking corporations, it was decided to issue a directive that would obviate the need for a banking

corporation to apply to the Department for a permit before any use of cloud-computing technologies; henceforth, a permit is needed only in cases specified in the Directive.

4. The Directive lays down guidelines and conditions for the use of cloud-computing technologies by a banking corporation, lists the cases in which banking corporations must obtain a permit from the Banking Supervision Department, and notes those in which banking corporations may use cloud-computing technologies without said permit. In any case, the Directive prohibits banking corporations using cloud-computing technologies for core activities and/or core systems.
5. Publishing a dedicated directive on cloud computing is designated to emphasize the need to manage the risks that inhere to any use of cloud-computing technologies by involving the highest managing echelons of the banking corporation. This Directive applies across the board to all kinds of cloud computing models, including those specified in Section 1 above.
6. After consulting with the Advisory Committee on Banking Business Affairs and with the approval of the Governor, I established the Proper Conduct of Banking Business Directive as specified below.

Structure of the Directive

7. The Directive is composed of seven chapters:
   (a) **Background**—including an introduction to the Directive and specification of its incidence;
   (b) **General**—general instructions;
   (c) **Corporate Governance**—expected involvement of the Board of Directors and Senior Management;
   (d) **Cloud-Computing Applications that Require a Permit**—cases in which a banking corporation must obtain a permit from the Banking Supervision Department before using cloud-computing technologies;
   (e) **Risk Management**—instructions pertaining to risk management and the application of cyber-defense and information-security measures for a banking corporation that needs a permit to use cloud-computing technologies;
   (f) **Contracting with a Cloud-Service Provider**—instructions pertaining to contracting with a cloud-service provider by a banking corporation;
   (g) **The Permit Letter**—matters that may be included in the permit letter to a banking corporation.
   (h) **Appendix A—Risk Assessment: Examples of Cloud-Computing Aspects—**examples of risks that should be taken into account when a risk assessment is performed.

Introduction and incidence (Sections 1–4 of the Directive)

8. The Directive notes the advantages of using cloud-computing technologies along with the risks inhering to their use. One of the main risks originates in the difficulty that a banking corporation faces in maintaining adequate command and control of cloud applications and of cyber-defense and information-security measures. In the Directive, it is stated with emphasis that alongside the traditional risks, which grow in intensity when cloud-computing technologies are used, there are specific risks.
9. The Directive allows the Supervisor of Banks to lay down specific provisions that are different from those spelled out in the Directive and also, in unusual cases only, to allow a banking corporation to use cloud-computing technologies notwithstanding the provisions of the Directive; and this, in view of different developments that may occur in the banking system

and/or ongoing developments both in cloud-computing technologies and in cyber defense and information security tools that may have implications for compliance with certain instructions.

General provisions (Sections 5–9 of the Directive)

10. The Directive prohibits banking corporations using cloud services for core activities and/or core systems, as the banking corporation defines them.
11. In the event that a banking corporation stores, transfers, or processes information that it defines as "sensitive," it must ensure that the cloud-service provider maintains a level of protection that complies with the EU Data Protection Directive (Directive 95/46 EC). Banking corporations are asked to monitor updates to this Directive regularly and ensure that the provider complies with changing arrangements.
12. The Directive refers explicitly to several proper conduct of banking management directives that are relevant to cloud computing in respect of risk management and the implementation of protection and control measures to mitigate them. The Directive places special emphasis on Proper Conduct of Banking Business Directive no. 357 because cloud computing is a particular instance of outsourcing; accordingly, Sections 17, 18, and 30 of Directive 357 deserve emphasis.
13. The Directive refers banking corporations to statutes, regulations, and guidelines that are relevant to this Directive, e.g., privacy protection laws and regulations.

Corporate governance (Sections 10–13 of the Directive)

14. A banking corporation that considers the possibility of using cloud-computing technologies must present the matter to the Board of Directors for discussion before it places the application in use. In said discussion, the Board shall be asked to discuss the risks that inhere to this technology as presented to it, as well as the controls with which these risks are to be mitigated. The Board is expected to understand the implications of the materialization of the risks for the banking corporation and its customers and should be convinced that the controls address these risks satisfactorily.
15. In addition to the foregoing, the Board of Directors must instruct Senior Management to formulate and approve a policy document on cloud computing uses and must also discuss and approve said policy. The policy document should refer to various aspects including those specified in the Directive. Senior Management should ensure that the banking corporation operates in accordance with the policy approved.
16. In the event that a banking corporation intends to use a cloud-computing technology that requires a permit as set forth in the Directive, Senior Management or an appropriate management committee shall discuss the application before it is placed in use. In certain cases, for example, if the application is critical to the bank or exposes the banking corporation to material risks, the Board of Directors should discuss it as well.

Cloud-computing applications that require a permit (Sections 14–17 of the Directive)

17. The Directive specifies the cases in which a banking corporation must obtain a permit from the Banking Supervision Department before using cloud-computing technologies. The first case is when the application includes sensitive information. The banking corporation is expected to define what "sensitive" information is and classify it in accordance with the policy and rules that it has established. Sensitive information is not necessarily that which pertains solely to confidential customer or employee details; it also includes any other information in accordance with the banking corporation's policy, such as business information under defined rules. The

second case is when the disclosure of the information, even if it is not sensitive, may allow adversaries to attack or compromise the banking corporation. The third case occurs if the shutdown of the service for any reason whatsoever may impair the banking corporation's conduct and/or ability to serve its customers. The fourth case in which a permit is necessary occurs if the application includes protective measures that belong to the same type or family of solutions and the banking corporation has no additional measure on its premises. An example would be a banking corporation that intends to run its entire e-mail filtering system on the cloud.

18. A banking corporation does not need a permit in cases not specified above. Several examples: statistical data stored on the cloud for sundry analysis or marketing purposes, in which none of the data can reveal its owner's identity. A cloud informational site does not require a permit unless it contains information that is sensitive or may cause an attack on the banking corporation or harm it.
19. The Directive emphasizes that even in cases where the banking corporation does not need a permit, it must perform a risk assessment relating to all relevant aspects (e.g., all types of relevant risks—legal, compliance, cyber, business-continuity, etc.) on an ongoing basis. In said risk assessment, all relevant players at the banking corporation should be involved.
20. Farther on, the Directive presents a list of instructions that the banking corporation must obey when they intend to use a cloud-computing application that requires a permit. Compliance with these instructions is a prerequisite for use of the application.

Risk management (Sections 18–22 of the Directive)

21. Banking corporations must perform due diligence not only before contracting with a cloud-service provider but also periodically during the term of the contract. This check is meant, among other things, to assure the corporation of the provider's financial strength, its professionalism in the context at hand, and its experience in the cloud-service application and in similar services for other entities. In certain cloud applications, SaaS in particular, it is difficult (and at times impossible) to switch to another cloud-service provider with reasonable celerity in the case of termination or interruption of contracting with the current provider (for whatever reason). This explains the importance of this instruction.
22. The Directive stresses the need to perform a risk assessment for each cloud application (even if it does not require a permit). This assessment should be done on an ongoing basis and should refer to relevant changes—not only technological or business-related—at both the banking corporation and the cloud-service provider. The Directive emphasizes the need to relate, in addition to traditional outsourcing risks, to risks that are typical of cloud computing, and it gives examples of such risks in the appendix, e.g., regulatory risks, risks relating to handling of irregular events, and so on.
23. The Directive stresses the importance of not settling for the cloud-service provider's own monitoring activity; in any case, the banking corporation must monitor cyber and information-security incidents on its own, e.g., by transferring information about such incidents to its central monitoring system.
24. It is not sufficient to ensure that the cloud-service provider protects sensitive information that the banking corporation stores with it; instead, the banking corporation must also ensure that adequate protective measures are taken that will prevent, to the extent possible, an attack on the corporation via its interfaces with the provider.

25. A banking corporation must encrypt all information that it transmits electronically and that is stored on cloud-service provider's premises. However, given the possible effect of encrypting all information on the application processing (e.g., data retrieval), the Directive allows banking corporations to encrypt only information that the corporation classifies as sensitive, which, if exposed, may be harmful to it and its customers.
26. The Directive allows encryption keys to be kept on the premises of the cloud-service provider. However, given that storing them on the banking corporation's premises creates a strong control for protection of the information that is kept with the provider, the corporation is expected to keep the encryption keys on its premises to the extent possible, unless it finds out that this causes difficulties, for example, in implementing the application. In that case, the banking corporation must implement compensatory controls.

Contracting with a Cloud-Service Provider (Sections 23–24 of the Directive)

27. In its contract with a cloud-service provider, a banking corporation should ensure that the document include an option to terminate service unilaterally. The Directive demands that the provider undertakes to allow the banking corporation to cancel the contract at any time and in any event on which it decides, e.g., dissatisfaction with service, transfer the service to another provider, no further need for the service, and so on.
28. The instruction is meant to prevent a situation in which the banking corporation's data (not only sensitive data) continues to be stored on the provider's premises after the contract with the provider is terminated. Accordingly, in any case of termination of use of the service, the provider must undertake in the contract to transfer to the banking corporation the banking corporation's data in its possession and to delete said data from its servers so that they cannot be restored and retrieved through the provider in any manner. The Directive notes that these actions shall be taken "within a short period of time"; it is recommended that the banking corporation specify this period of time in the contract.
29. In the event that a banking corporation changes cloud-service providers or if its current provider undergoes a change in ownership, the banking corporation must review the contract to ensure that the new owner, too, will comply with the provider's obligations, including those in the Directive.

The Permit Letter (Sections 25–26 of the Directive)

30. The permit letter usually includes requirements in addition to those specified in this Directive. These additional requirements, which the corporation is expected to satisfy before placing the service in use, are specific and relevant to the specific cloud service for which the banking corporation applies for a permit.
31. Four requirements that are defined as across-the-board in the Supervisor's letter of June 29, 2015, are no longer specified as binding requirements in the Directive. However, the need to specify these requirements will be reviewed when the banking corporation applies for a permit, as the case may be; if the Banking Supervision Department decides that the requirement is relevant for the cloud use that the banking corporation wishes to apply, it will be included in the permit letter. The Directive spells out the four matters that pertain to said requirements.

Effect

32. The contents of this circular shall go into effect immediately.

Update of file

33. Update pages for the Proper Conduct of Banking Business Directive file are attached. The provisions of the update follow.

Remove page	**Insert page**
———	362-1-6 (7/17) [1]

Respectfully,

Dr. Hedva Ber
Supervisor of Banks