

Bank of Israel
Banking Supervision Department
Technology and Innovation Division

June 13, 2022

Circular Number C-06-2715

Attn:

Banking Corporations

Re: Cloud computing

(Proper Conduct of Banking Business Directive no. 362)

Introduction

1. Cloud-computing services enhance and amplify organizational computer abilities and allow organizations, including banking corporations, to improve their efficiency and respond quickly to market needs. Cloud-computing technology has been developing rapidly but still carries unique risks, and for this reason, may expose the banking corporation to heightened operational risks in fields such as information-security and cyber, business-continuity, and reputation. This Directive is aimed at guiding the management of these risks, among other purposes.
2. The Banking Supervision Department considers the use of cloud-computing services as a specific case of outsourcing, and therefore, banking corporations that use cloud-computing services must apply, apart from the instructions in this Directive, all instructions in Proper Conduct of Banking Business Directive 359A, “Outsourcing” (hereinafter: Directive 359A), with certain exceptions (see further details in Appendix A, “Appendix A—Incidence of Directives 362 and 359A for Material and Non-Material Cloud-computing”).
In accordance with the foregoing, the considerations spelled out in Section 27 of Directive 359A, used there to define the level of materiality in outsourcing, are invoked, and additional considerations for materiality are added as specified in the definition of “material cloud-computing” that appears in this Directive. Also, the terminology in the Directive has been harmonized with that of Directive 359A, such that the word “supplier” is replaced with “service provider” and “contractual agreement” is replaced with the word “contract.”
3. Banking corporations must have a policy on the use of cloud-computing services in place, determining *inter alia* the characteristics of services defined as “material cloud-computing” in view of the aforementioned considerations and risk management in using cloud-computing services generally. Consequently, the use of the term “core systems” is eliminated as is the injunction against banking corporations’ use of cloud computing for core systems. A banking corporation shall anchor said policy in a document titled “Use of Cloud-Computing Services Policy,” which shall be presented to the Board of Directors for its approval.
4. As stated, cloud computing is a specific case of outsourcing, yet the use of which entails specific requirements that are not typical of all outsourcing and are not spelled out in Directive 359A.

This Directive specifies the unique requirements that attend to the use of cloud-computing services in various matters including corporate governance, risk management, contracting with a cloud-computing service provider, information security and cyber defense, and business continuity.

5. This measure joins the other steps that the Banking Supervision Department has taken in recent years to bring banking system in Israel into line with the competitive and changing world and with technological progress.
6. After consulting with the Advisory Committee on Banking Business Affairs and with the approval of the Governor, I have amended this Directive as detailed below.

Amendments to Directive 362

Chapter A—Background

Incidence

7. Section 5

It is stated for clarity that this Directive does not apply to a “private cloud” as defined in Section 6 of the Directive; however, outsourcing with a private cloud is subject to Proper Conduct of Banking Business Directive 359A, “Outsourcing”.

Chapter B—General

Definitions

8. Section 6

8.1 The terms “cloud-computing”, “private cloud” and “material cloud-computing” are defined.

8.2 A definition of “cloud computing” based on the EBA¹ and NIST² definitions (the NIST Definition of Cloud Computing) is added.

8.3 A definition of “private cloud” based on the NIST definition was added. By and large, one may characterize a private cloud as a cloud-computing infrastructure reserved for the exclusive use of one banking corporation. Such an infrastructure may be operated by the organization or an outside service provider and may be located on the premises of the banking corporation or elsewhere (e.g., the computer center of a traditional bank, situated in the building of the bank or in another outsourced building).

8.4 A definition of “material cloud-computing” is added. It is based on the definition of “outsourcing” in Directive 359A, and considerations relating to the cloud deployment model (public, community, hybrid, etc.) and the cloud-computing service model (SaaS, PaaS, IaaS, etc.) are added to the considerations for determining the materiality of cloud-computing activity, enumerated in Section 27 of Directive 359A.

Several considerations that appeared in Appendix A of the version that exists in Circular 2669 as examples of material cloud-computing are also added to the definition.

¹ European Banking Authority.

² The National Institute of Standards and Technology.

General instructions

9. The injunction against using cloud-computing services for core activities and/or core systems is cancelled.

10. Section 7

The Section is updated in accordance with the European regulation in effect: the General Data Protection Regulation (GDPR) of the European Union.

11. Section 8

11.1 This Section establishes the rule by which cloud computing is a specific case of outsourcing. Accordingly, insofar as material cloud-computing as defined in the Directive is at issue, Directive 359A shall apply to it. An exception to this rule is Section 33 of Directive 359A, concerning compulsory reporting to the Supervisor of Banks, which shall not apply to cloud computing whether it is material or not.

11.2 It is stated for emphasis that in deciding on whether cloud-computing is material, a banking corporation must consider, in addition to the considerations listed in Section 27 of Directive 359A, additional aspects unique to cloud-computing that appear in the definition of “material cloud-computing” in this Directive. (See Section 8.4 of this Circular.)

11.3 Mention of the need to keep cloud computing in compliance with the instructions of the Proper Conduct of Banking Business Directives specified in the Section is cancelled. Said cancelation of mention of these directives shall not derogate from the banking corporation’s need to comply with them or with any other relevant instruction in a Proper Conduct of Banking Business Directive in the context of cloud-computing.

12. Section 9

Registrar of Databases instruction 2/2011—“Use of Outsourcing Services for Processing of Personal Information”—establishes the scope of its incidence for entities supervised by the Supervisor of Banks; therefore, mention of this instruction in the Directive is canceled.

13. Section 10

13.1 The ability of consulting with experts to mitigate risks in cloud-computing is not unique to this topic and is cancelled in order to prevent banking corporations from inferring that such consultation is not possible except where explicitly stated in the Directive.

13.2 A requirement is added to the effect that a banking corporation must ensure a cloud-computing service provider’s accountability to the banking corporation, including the performance of its contractual obligations to the banking corporation and including a case in which the cloud-computing service provider uses a secondary service provider.

Chapter C—Corporate Governance

14. Section 11

As stated in Section 11 of this Circular, this Section is an exception to the rule established in Section 8 of the Directive, by which Directive 359A shall apply only in cases of material cloud-computing. It is stated in this Section that the instructions in Directive 359A that are relevant in respect of corporate governance (as are spelled out in Chapter B of Directive 359A) shall also apply in cases of non-material cloud-computing, with the exceptions of Sections 13(c) and 16.

Board of Directors

15. Sections 12–14

As stated in Section 11 of this Circular, cloud computing is a specific case of outsourcing that has unique characteristics. Accordingly, unique requirements for the Board of Directors are added in the context of using the cloud-computing services specified in this Section that do not appear in Directive 359A.

Senior management

16. Section 15

As stated in Section 11 of this Circular, cloud computing is a specific case of outsourcing that has unique characteristics. This Section spells out the unique obligations of senior management in the context of using cloud-computing services that do not appear in Directive 359A.

The policy that senior management shall formulate, entailing the approval of the Board of Directors, shall distinguish between the use of material cloud-computing services, which requires the approval of the Board of Directors, and the use of cloud-computing services that require the approval of senior management and those requiring the approval of some other entity. The policy shall be consistent with the various regulatory requirements, including those relating to ICT, information security and cyber defense, business continuity, and operational risk management.

17. Section 16

Matters unique to the use of cloud-computing services, to which the policy established by a banking corporation must relate, are added.

18. Section 17

Senior management shall monitor the implementation of the “Use of Cloud-Computing Services Policy” document on a regular basis.

19. Sections 18–19

19.1 Cloud computing has unique characteristics and, as stated in Section 1 of this Circular, its implementation may expose a banking corporation to heightened operational risks. Accordingly, banking corporation must prepare appropriately along the first and second lines of defense when it begins to use cloud-computing services.

19.2 Within the framework of the first line of defense, an officer subordinate to the Chief Information Officer (CIO), thoroughly familiar with the risks attending to the use of cloud-computing services and the technological services given by all providers of cloud-computing services with which the banking corporation has contracted, shall be designated. In addition, the banking corporation shall consider, depending on the circumstances, the

need to place an officer in charge of every cloud-computing service provider with which it has contracted.

- 19.3 Within the framework of the second line of defense, an officer subordinate to the Chief Risk Officer (CRO) shall be designated to be in charge of ongoing thorough assessment of the risks of cloud computing to overall activity from the broad perspective of all cloud-computing services that the banking corporation receives.

20. Section 20

Senior management shall draw up a multiyear work plan for cloud computing. It shall include, among other things, the inherent risks of cloud-computing services and the controls that are being applied, or are intended to be applied, to mitigate them.

Chapter E— Risk Management

21. Section 21

21.1 This Section (Section 17(a) in the version existing in Circular 2669) is essentially transferred to Section 23 of this Directive.

21.2 This Section creates an exception to the rule established in Section 8 of this Directive by applying Directive 359A only to cases of material cloud-computing. In this Section, it is stated that the instructions in Directive 359A that are relevant to risk management (Sections 24–26 of Directive 359A) shall also apply in cases of cloud-computing that is not material.

22. Section 22

This Section (Section 18 in the version existing in Circular 2669) is essentially transferred to Chapter F, “Contracting with a Cloud-Service Provider.” The matter of due diligence is included in Section 29 of this Directive.

23. Section 23

The following are added:

23.1 (a) Reference to main aspects that should be taken into account in the risk assessment, which are specified in Appendix B of this Directive—“Main Aspects of Cloud-Computing Risk Assessment.”

23.2 (b) A compulsory risk survey of material cloud computing, as set forth in Proper Conduct of Banking Business Directive 350, “Operational Risk Management,” to be carried out at least once every two years.

23.3 (c) Compulsory verification of the existence of appropriate compensatory controls in accordance with the risk assessment.

24. Section 24

24.1 This Section (Section 20 in the version existing in Circular 2669) is transferred to Chapter G1, “Information Security and Cyber Defense.”

24.2 The requirement of including specific reference to cloud-computing risks in regular reports to senior management and the Board of Directors concerning operational risks, as required under Proper Conduct of Banking Business Directive 350, is added.

25. Section 25

25.1 This Section (Section 21 in the version existing in Circular 2669) is transferred to Chapter G1, “Information Security and Cyber Defense.”

25.2 The requirement of defining responsibilities for management, control, approval and documentation of cloud-computing services at a banking corporation and the requirement of creating a model for the apportionment of responsibilities between a banking corporation and a cloud-computing service provider are added. It should be emphasized, however, that a banking corporation remains responsible for complying with all laws and directives that apply to it and it is solely accountable to its customers and to the Banking Supervision Department.

26. Sections 26–27

26.1 This Section (Section 22 in the version existing in Circular 2669) is transferred to Chapter G1, “Information Security and Cyber Defense.”

26.2 The requirement of documenting and updating the aspects of cloud-computing services specified in the Directive is added.

Chapter F—Contracting with a Cloud-Service Provider

27. Section 28

To eliminate doubt, it is stated that Chapter F of this Directive, “Contracting with a Cloud-Service Provider”, shall not apply to banking corporations in cases of cloud computing that are not material.

Due diligence

28. Section 29

28.1. Additional aspects for compulsory inclusion in due diligence on a cloud-computing service provider before contracting with it takes place, in addition to those specified in Directive 359A, are spelled out in this Section:

(a) The service provider’s compliance with all relevant laws and regulations for the use of cloud-computing technologies, including privacy-protection laws in effect the state in which it operates;

(b) Assurance of an adequate level of cyber defense in accordance with criteria that the banking corporation shall specify, e.g., reporting and reports from the cloud-computing service provider, intelligence information about past events at the cloud-computing service provider, etc.

28.2. The matters specified in this Section constitute a basic list for due diligence; it is stated for clarity that the list is not exhaustive.

The cloud-computing contract

29. Section 30

- 29.1. (a) Given that in Section 8 of this Directive, concerning material cloud-computing, the sections of Directive 359A shall apply as stated, and since the instructions in said Section appear in Section 23(h) of Directive 359A, this Section in its full wording is canceled. However, emphasis is placed on deleting the banking corporation's information, or taking similar action, from the systems of the cloud-computing service provider and receiving the assurance of the cloud-computing service provider that this information cannot be retrieved from its systems.
- 29.2. (b) Given that, as stated in Section 8 of this Directive, the provisions of Directive 359A shall apply to a cloud-computing service provider and the instructions spelled out in said Section appear in Section 23(f) of Directive 359A, this Section is canceled.
- 29.3. (c) Given that, as stated in Section 8 of this Directive, the provisions of Directive 359A shall apply to a cloud-computing service provider and the instructions spelled out in said Section appear in Section 23(f) of Directive 359A, this Section is canceled.
- 29.4. (d) The Section is deleted and, instead, a requirement is added: assurance of the banking corporation's ability to receive information of relevance for the activities that it transfers to the outsource service provider, including audits of the service provider, and examination of said information or sharing thereof it with the Supervisor of Banks at the Supervisor's request.
- 29.5. It should also be noted that Section 22 of Directive 359A, concerning assuring the ability of the Supervisor of Banks to wield his or her powers, shall apply to material cloud-computing.
- 29.6. (e) The undertakings of a cloud-computing service provider, as set forth in the model concerning the apportionment of responsibilities of the banking corporation as required by Section 25 of the Directive, shall be enshrined in the contract.
- 29.7. (f) The location of the cloud facility where service is given and that of where the data are stored, including the cloud-computing service provider's undertaking to apprise the banking corporation of any change therein, shall be noted in the contract.
- 29.8. (g) The contract shall include reference to the manner in which sensitive information will be stored and accessed during and after the term of service.
- 29.9. (h) The contract shall include reference to information backup and to the possibility of information retrieval.
- 29.10. (i) The following shall be defined in the contract: the banking corporation's ability to activate or deactivate material cloud-computing services or components thereof, including blockage of access, insofar as is relevant and in a state of emergency, e.g., a cyber incident, due to the need to mitigate risks—either independently or by the cloud-computing service provider at the request of the banking corporation; and the processes that support these abilities, with reference to resources of the cloud-computing service provider that the banking corporation uses jointly with other clients of the same cloud-computing service provider.

- 29.11. (j) The insertion of a requirement that the cloud-computing service provider participate in cyber exercises that the banking corporation will hold on a periodic basis, commensurate with the nature of the application, should be considered.
- 29.12. (k) The contract shall include reference to the implementation of compensatory controls in accordance with the risk assessment specified in Section 23 of this Directive.
- 29.13. The matters specified in this Section constitute a basic list in any contract with a cloud-computing service provider; to make matters clear, it is stated that the list is not exhaustive.

Management of contractual relations with a material cloud-computing service provider

30. Section 31

- 30.1. The Section is expanded and specifies the actions that a banking corporation must take during the term of its contract with a provider of material cloud-computing services (Subsections (a)—(e)).
- 30.2. In Subsection (f), a banking corporation is also required to review the need to update the contract with the service provider at least once every three years or upon the occurrence of a material incident or change in the cloud-computing services or a change in any law or regulation of relevance for the use of cloud-computing technologies or services;
- 30.3. The contents of this Section (Section 24 in the version existing in Circular 2669), concerning change of ownership of a cloud-computing service provider, are included in Subsection (g). The term “ownership” is changed to “controller” in order to extend the Section to the case of a public company.

Chapter G1—Information Security and Cyber Defense

31. To eliminate doubt, the Information Security and Cyber Defense chapter applies to all cloud-computing, material or not.

32. Sections 32–33

These sections were transferred from Section 22 of the version that exists in Circular 2669 and were updated in respect of aspects of the requirement that a banking corporation, in managing information-exposure risk, shall make reference, *inter alia*, to aspects of information classification, location of encryption keys, banking-corporation involvement in managing encryption keys and encryption level, encryption methods, etc.

33. Section 34

This section was transferred from Section 20 of the version that exists in Circular 2669. Special emphases on monitoring cyber incidents while using cloud-computing services can be found in Appendix C of this Directive, “Monitoring Cyber Incidents in Cloud-computing.” Said monitoring should be carried out in a way that will make it possible to detect a cyber incident as early as possible and in a manner relevant to the type of cloud-computer service model given (SaaS, PaaS, IaaS, etc.).

34. Section 35

A Section about coping with a cyber incident in cloud-computing services, including holding cyber exercises that place unique emphases on the banking corporation's preparedness for cyber incidents in these services, is added.

35. Section 36

This Section was transferred from Section 21 of the version that exists in Circular 2669.

Chapter G2—Business Continuity

36. Section 37

Insofar as cloud computing is a critical service for the banking corporation, the relevant requirements in Proper Conduct of Banking Business Directive 355 shall apply to it.

37. Section 38

Insofar as cloud-computing service is given in a location other than Israel, a banking corporation shall examine plans for response to a scenario of service unavailability due to disruption of communication or geopolitical events vis-à-vis a foreign country. The corporation shall also assess the service provider's ability to maintain business continuation amid local attribution threats of the host country.

38. Section 39

At a main or alternate cloud-computing site, a banking corporation must make sure that the site complies with the Tier3 requirements of the UpTime Institute (UTI) standards by obtaining a certificate from UTI or an outside opinion from an independent expert.

Chapter H—Reporting to Banking Supervision Department

39. Section 40

39.1. Once per year, at the end of a calendar year, a banking corporation shall present the Banking Supervision Department with a written report carried out on the basis of Reporting to Banking Supervision Directive No. 881, "(Annual) Reporting of Cloud Computing." It is stated for clarity that continuity of reportage between the reporting requirement in Circular 2669 and that established in this Circular will apply in any case.

39.2. It is emphasized that, as stated in Section 8 of this Directive, Section 33 of Directive 359A shall not apply to material cloud-computing and a banking corporation need not serve the Supervisor of Banks with advance notice of the implementation of material cloud-computing, explaining the reason for outsourcing said activity to cloud-computing, as close as possible to a decision to this effect at the senior-management level.

Appendix A—Examples of Material Cloud-computing

40. The Appendix is canceled because the examples presented in it were transferred as additional considerations for examination under the definition of “Material Cloud-computing”; see Section 8 in this Circular, “Definitions.”

Appendix B—Main Aspects in the Evaluation of Cloud-Computing Risks

41. The Appendix includes main aspects of the risk assessment in cloud computing. Below are the main amendments that were made in the Appendix:

- 41.1. Aspects that appear in Directive 359A are deleted.
- 41.2. Systemic risk is deleted.
- 41.3. (b) Reference to risk aspects originating in the use or non-use of a multi-configuration cloud (cloud infrastructures based on a combination of several different cloud-computing solutions), such as distribution among several cloud-computing service providers, including professional implications against concentration of receiving cloud-computing services from one computer-service provider, is added.
- 41.4. (e) Reference to risk aspects associated with receiving cloud-computing service from a provider of information-security and cyber-defense measures as a sole layer of defense, is added.
- 41.5. (g) Reference to risk aspects associated with changes that the cloud-computing service provider must make as the result of technological developments and changes in the services delivered is added.
- 41.6. (k) Aspects associated with ongoing operational risks (including support personnel, working processes, incidents management, etc.) and mitigation of such risks by settling responsibilities between the banking corporation and the cloud-computing service provider are expanded.
- 41.7. (n) Reference to maintaining logical and administrative separation of different customers’ systems in the cloud is added.

Appendix C—Monitoring Cyber Incidents in Cloud-computing

42. Management and definition of monitoring shall comport with the various service model types (e.g., PaaS, SaaS, and IaaS), with the banking corporation expected, at the very least, to manage and define rules, receive logs, and acknowledge existing rules from which it shall make inferences in regard to integrating additional rules into its monitoring systems.

The monitoring shall include, among other things, deviations from legitimate activity in the banking corporation’s infrastructure associated with the cloud-computing service. The monitoring tools shall meet accepted standards and shall be integratable into the existing monitoring systems of the banking corporation. The banking corporation shall specify control operations for the continued continuity of monitoring of a material cloud-computing service at such time as communication between the banking corporation and the monitoring system of the cloud environment is disrupted.

Effective date and transition provisions

- 43. The contents of this Directive will go into effect on January 1, 2023.
- 44. For contracts executed before the promulgation of this Directive—on the next date of renewal of the contract and no later than four years from the effective date, a banking corporation shall align the contracts with this Directive where necessary.
- 45. For contracts executed after the promulgation of this Directive up to the effective date—no later than one year after the effective date, the banking corporation shall align its contracts with this Directive where necessary.
- 46. A banking corporation may apply this directive in its entirety before the effective date.
- 47. From the effective date of this Directive, Section 29 of Proper Conduct of Banking Business Directive 480 "Adjustments to Proper Conduct of Banking Business Directives that apply to New Banking Corporations" is canceled.

Treatment of existing permits

- 48. On the effective date of this Directive, permits or authorizations issued for a service defined as a cloud-computing service in this Directive:
 - (a) when said authorization or permit includes terms or conditions that are not required under this Directive, said terms or conditions are canceled.
 - (b) when said authorization or permit includes terms or conditions that clash with the principles of the Directive, action shall be taken in accordance with Section 44 of this Circular.

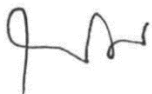
File update

- 49. Update pages for the Proper Conduct of Banking Business Directives file are attached. The following are the update instructions:

Remove page
362-1-10 [3] (9/21)

Insert page
362-1-15 [4] (6/22)

Sincerely,



Yair Avidan
Supervisor of Banks

**Appendix A—Application of Directives 362 and 359A
for Material and Non-Material Cloud-computing**

362		
Principle: Directive 362 applies to all cloud computing (material and non-material) unless otherwise stated in the Directive.		
	Non-material cloud-computing	Material cloud-computing
Chapter A—Background (Introduction, Application)	Yes	Yes
Chapter B—General (Definitions, General Instructions)	Yes	
Chapter C: Corporate Governance (Board of Directors, Senior Management)	Yes	
Chapter E: Risk Management	Yes	
Chapter F: Contracting with a Cloud-Service Provider (Due Diligence, the Cloud-Computing Contract, Management of Contractual Relations with a Material Cloud-Computing Service Provider)	No	
Chapter G1: Information Security and Cyber Defense	Yes	
Chapter G2: Business Continuity	No	
Chapter H: Reporting to Banking Supervision Department	Yes	
359a		
Principle: Directive 359A applies to material cloud-computing with the exception of compulsory reporting in Section 33). In certain chapters, where this is noted explicitly in Directive 362, Directive 359A also applies to non-material cloud-computing.		
	Non-material cloud-computing	Material cloud-computing
Chapter A: General Remarks (Introduction, Application, Definitions)	Yes (except for Definitions)	Yes
Chapter B: Corporate Governance (Board of Directors, Senior Management, Internal Audit)	Yes, except for Sections 13(c) and 16	Yes
Chapter C: Restrictions on Outsourcing (Operations that May Not Be Outsourced)	No	Yes
Chapter D: Contracting with a Service Provider (Due-Diligence Check of a Service Provider, Outsourcing Contract)	No	Yes
Chapter E: Management of Outsourcing Risk (Outsourcing Management Plan, Business Continuity Plan)	Sections 24–26: Yes (in the context of risk management); Section 27: yes (in the context of determining level of materiality). Sections 28–29: no.	Yes

Chapter F: Outsourcing of Special Activities (Contracting with Service Provider Who Works with Customers, Outsourcing of Internal Auditing Activity, Outsourcing Associated with Compliance and Prohibition of Money Laundering and Terror Financing)	No	Yes
Chapter G: Reporting to the Banking Supervision Department (Compulsory Reporting to the Supervisor of Banks)	No	Section 33—no Section 34—yes
Chapter H: Effective date and Transitional Provisions (Effective date and Transitional Provisions, Treatment of Existing Directives and Permits)	No	Yes, for cloud-computing services defined as material under the definition of outsourcing in Directive 359A.

* Wherever the wording in this Appendix clashes with that in Directives 362 and 359A, the wording in the directives shall prevail.