Directive 362—Cloud Computing
Chapter A: Background

Introduction

1. Moving to various forms of cloud computing has become a growing trend in recent years. These technologies make it possible to use computer resources efficiently and easily, and to share resources and use them as necessary. This comes hand-in-hand with savings in hardware costs, data-center space, electricity, and so forth. The use of cloud-computing services by banks around the world, and in Israel, may offer a response to business needs such as material system upgrades. The trend is expected to accelerate, for reasons including the development and upgrading of cloud-computing technologies and the acceleration of competition among banks.
2. Notwithstanding its advantages, cloud technologies may expose a banking corporation to material operational risks associated with information security and cyber defense, business continuity, command and control of IT assets, and other issues. These risks originate, *inter alia*, in dependency on specific service providers or technologies; suboptimal implementation of management, security, and command-and-control tools; difficulties in protecting information and applying adequate controls; intensification of potential damage in the event of a failure, particularly when single points of failure come about; and other matters. Notably, some of these risks are known but the unique characteristics of these technologies create special risks of their own.
3. It is the supervisory approach toward aspects of technology, information security, and cyber defense to be a business enabler and to regard the transition of banking corporations' systems to cloud computing, including material systems, as a part of technological innovation and development—all of which, subject to intelligent, cautious, and meticulous risk management.

Application

4. (a) This Directive shall apply to banking corporations as defined in the Banking (Licensing) Law, 5741-1981 (hereinafter in this Directive—"banking corporation"):
    1) a banking corporation;
    2) a banking corporation as set forth in Sections 11(a) (3a) and (3b);
    3) a banking corporation as set forth in Section 11(b);
    4) a merchant acquirer as set forth in Section 36(i).

    (b) Cancelled.

5. This Directive does not apply to a "private cloud" as defined in Section 6 of this Directive.

Chapter B: General

6. The following definitions are used in this Directive:

"Cloud computing"	A model for enabling ubiquitous, convenient on demand network access to a shared pool of configurable computer resources (e.g., networks, servers, storage, applications, and services) that can be rapidly adjusted.
"Private cloud"	The cloud infrastructure is provisined for exclusive use by a single banking corporation. It may be owned, managed, and operated by the banking corporation, a third party, or some combination of them, and may exist on or off premises.
"Material cloud-computing"	Use of outsourced cloud-computing services in the sense of this term in Section 8 of Proper Conduct of Banking Business Directive 359A, "Outsourcing" (hereinafter: Directive 359A); for this purpose, the materiality of cloud-computing activity is determined on the basis of the

considerations specified in Section 27 of Directive 359A and in view of the following additional considerations:

(a) the cloud-computing deployment model;

(b) the cloud-computing service model;

(c) the inclusion in the cloud-computing service of information that the banking corporation defines as sensitive;

(d) the inclusion of information that the banking corporation does not define as sensitive but its exposure allows one to infer details that will make it possible to attack or harm the banking corporation or its customers;

(e) the cloud-computing service provides information-security and cyber-defense measures as the sole layer of defense, with no similar measures taken on the banking corporation's premises.

General instructions

7. A banking corporation shall not store, transfer, or process information that it defines as "sensitive" (e.g., customer data, confidential business information, etc.) on a cloud outside the borders of the State of Israel unless it has ascertained that the cloud-service provider maintains a level of protection that complies with the European Union General Data Protection Regulation (GDPR).
8. Material-cloud-computing services shall be considered a material outsourcing activity and, as such, are subject to Directive 359A (excluding compulsory reportage under Section 33 of Directive 359A) as well as to this Directive, which specifies and elaborates on the guidelines specific to them. Accordingly, the definitions that appear in Directive 359A are also relevant to this Directive.
9. Nothing in this Directive shall derogate from the obligations applying to a banking corporation under all relevant laws and regulations for the use of cloud-computing technologies, including the Privacy Protection Law and the Privacy Protection

Regulations (Transfer of Information to Databases Outside the Borders of the Country), 5761-2001.

10. A banking corporation shall ascertain that its cloud-computing service provider is accountable to the banking corporation, including carrying out 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

11. Chapter B of Directive 359A, concerning corporate governance, shall also apply to cloud computing that is not material cloud computing, with the exceptions of Sections 13(c) and 16 of Directive 359A.

Board of Directors

12. The Board of Directors shall discuss and approve the document titled "Use of Cloud-Computing Services Policy," as is discussed in Section 16 below.
13. The Board of Directors shall approve the multiannual work plan for cloud computing as set forth in Section 20 below, including the implementation of any material cloud-computing service.
14. The Board of Directors shall verify that the use of cloud computing complies with the policy established as aforesaid.

Senior management

15. Senior management shall formulate a cloud-computing policy that will delineate, *inter alia*, the characteristics of services defined as material cloud computing that require the approval of the Board of Directors, those that require the approval of senior management, and those that require the approval of some other entity.
16. The document titled "Use of Cloud-Computing Services Policy" shall relate to determining the level of materiality of cloud-computing services on the basis of the definition of material cloud computing in this Directive, the authorities, responsibilities and actions of cloud-computing service management entities

including managing the cloud-computing service provider, controls and control entities, the characteristics and scope of services, approval processes and approval echelons, and the responsibilities of various entities at the banking corporation for handling legal, maintenance, monitoring, information security and cyber defense, incident handling, business continuity and functional continuity, etc. Said policy shall also respond to the requirements set forth in this Directive and in other relevant directives.

17. Senior management shall monitor, on a regular basis, the implementation of the "Use of Cloud-Computing Services Policy" document as approved by the Board of Directors.
18. A banking corporation shall designate an official subordinate to the Chief Information Officer (CIO) who will become thoroughly familiar with the risks and the technological services of every cloud-computing service provider with which the banking corporation contracts. The banking corporation shall consider the need to nominate an officer in charge of each cloud-computing service provider with which it has contracted.
19. A banking corporation shall designate an officer subordinate to the Chief Risk Officer (CRO) who will become thoroughly familiar with the risks of all aspects of activity in cloud computing.
20. Senior management shall prepare a multiyear working plan for cloud computing that will respond, *inter alia*, to the inherent risks of the cloud-computing services and the controls that are being applied, or are intended to be applied, to mitigate them.

Chapter D: Cloud-Computing Implementations that Require a Permit—Cancelled

Chapter E: Risk Management

21. Sections 24–26 of Directive 359A shall also apply to cloud computing that is not material.
22. Canceled.
23. A banking corporation shall perform a risk assessment and a risk survey in the following manner:
    (a) risk-mapping and risk-assessment for each material cloud-computing service implementation. The risk assessment shall be performed before the contract is concluded with the cloud-computing service provider and shall be updated regularly during the term of the contract, *inter alia* in accordance with technological, legal, regulatory, business, and organizational changes, among others, at the banking corporation and at the cloud-computing service provider. Even though cloud computing is a distinct case of outsourcing, the risk assessment should also include specific risks (technological and other) associated with its use. Main aspects to be taken into account appear in Appendix B, "Appendix B—Main Aspects of Cloud-Computing Risk Assessment."
    (b) In cases of material cloud-computing services, a risk survey as set forth in Proper Conduct of Banking Business Directive 350, "Operational Risk Management," shall be performed at least once every two years.
    (c) The banking corporation shall verify that it has in place appropriate compensatory controls in accordance with the risk assessment.
24. The regular reports presented to senior management and the Board of Directors in regard to operational risk matters, as set forth in Proper Conduct of Banking Business Directive 350, "Operational Risk Management," shall include specific reference to cloud-computing risks.
25. A banking corporation shall define the following:
    (a) responsibilities for management, control, approval, and documentation of its cloud-computing services in the banking corporation.

(b) a model for the apportionment of responsibilities between the banking corporation and the cloud-computing service provider, including information-security and cyber-defense aspects. Said apportionment of responsibilities shall not derogate from the banking corporation's responsibility for complying with all laws and directives that apply to it.

26. For each cloud-computing service, the banking corporation shall document the following aspects at the very least:
    (a) the decisions and considerations behind the implementation of cloud-computing services, such as level of materiality, considerations in favor of the use of cloud services, risks, approvals, and so on.
    (b) characteristics of the cloud-computing service provider in the contract therewith, such as date of contract execution, renewal, and options of extension, location of cloud and data-storage facilities, service model and cost of service, jurisdictional powers, and so on.
    (c) characteristics of the cloud-computing services, such as mapping and description of the architecture, interfaces, information-security and cyber-defense requirements, etc.
27. A banking corporation shall update the documentation enumerated in Section 26 *supra* in any case of change in one of the characteristics specified in said Section. Also, on a periodic basis that shall be established, the banking corporation shall ensure that said documentation is up to date.

Chapter F: Contracting with a Cloud-Service Provider

28. This Chapter does not apply to non-material cloud computing.

Due diligence

29. In material cloud computing, the banking corporation shall perform due diligence on the cloud-computing service provider, including identifying and assessing potential risks in contracting with it and using its services, as set forth in Section 23, and at

least in accordance with the risks enumerated in Appendix B of this Directive, "Main Aspects of Cloud-Computing Risk Assessment." In addition, the banking corporation shall examine:

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

(b) assurance of an adequate level of cyber defense as set forth, *inter alia,* in the "Use of Cloud-Computing Services Policy" document.

The cloud-computing contract

30. Without derogating from the obligations applying to a banking corporation under Proper Conduct of Banking Business Directive 359A and Proper Conduct of Banking Business Directive 363, "Supply Chain Cyber Risk Management," in material cloud computing, the contract with the cloud-computing service provider shall include reference to the following matters among others:

(a) deletion of the banking corporation's information, or a similar operation, from the systems of the cloud-computing service provider, and assurance from the provider that this information cannot be retrieved from its systems.

(b) canceled.

(c) canceled.

(d) assurance of the banking corporation's ability to receive relevant information for its activities that it transferred to the outsource service provider, including audits of the service provider, and to examine it or share it with the Supervisor of Banks at the Supervisor's request.

(e) implementation of the guidelines of the model of apportionment of responsibilities set forth in Section 25.

(f) the location of the cloud facility where the service will be provided and the location of data storage, including an undertaking by the cloud-computing service provider to apprise the banking corporation, in advance, of any change therein;

(g) the manner in which sensitive information will be stored and accessed during and after the term of service;

(h) information backup and the possibility of information retrieval;

(i) definition of 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. definition of 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 service provider;

(j) examining the insertion of a requirement that the cloud-computing service provider will commit to participate in cyber exercises that the banking corporation will hold on a periodic basis commensurate with the nature of the application.

(k) application of compensatory controls that the cloud-computing service provider needs to provide in accordance with the risk assessment specified in Section 23 of this Directive.

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

31. A banking corporation shall base the management of its contractual relations with a cloud-computing service provider of material cloud-computing service on the following principles:

(a) monitoring of service performance, security and information security, and attainment of the service levels agreed upon with the cloud-computing service provider, all by using monitoring means that comply with the banking corporation's risk appetite;

(b) evaluating arrangements with the cloud-computing service provider in relation to risk situations, incidents, and changes that occured during the contract term,

and in relation to critical operation of the banking corporation's computer systems in the cloud. Said assessment shall also include a risk assessment and shall take into account the cloud-computing service provider's abilities and compliance with requirements in respect of technology, business continuity, and information security and cyber defense;

(c) monitoring implementation of the apportionment-of-responsibilities model set forth in Section 25;

(d) managing permanent and ongoing interfaces of the banking corporation's business-continuity manager and the cyber-defense manager with those at the banking corporation who are responsible for ongoing relations with the cloud-computing service provider, including clear definition of their roll and duties within the framework of these interfaces.

(e) having a plan in place for exit or termination of contract. reviewing and updating the said plan once every three years;

(f) reviewing the need to update the contract with the cloud-computing 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 laws or regulations of relevance for the use of cloud-computing technologies or services;

(g) Whenever the cloud-computing service provider undergoes a change of control, the banking corporation shall review the contract to ensure that the new controller, will also comply with the cloud-computing service provider's obligations.

Chapter G: The Permit Letter—Cancelled

Chapter G1: Information Security and Cyber Defense

32. A banking corporation shall manage information-security and cyber-defense risks in cloud computing (material and non-material) with 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. The banking corporation's information must be encrypted when transferred over communication media and when placed in storage. In cases where the banking corporation finds it difficult to encrypt all said information, it should encrypt at least the data that it has classified as sensitive information or that may harm the banking corporation and its customers if exposed.
34. A banking corporation shall make sure that it has the ability to perform uninterrupted, full, and real-time monitoring in a way that will allow it to detect a cyber incident as early as possible and that is relevant to the cloud-computing service model given, this in respect of cyber incidents (as defined in Proper Conduct of Banking Business Directive 361, "Cyber Defense Management") that are associated with cloud-computing services *inter alia*, as specified in Appendix C of this Directive, "Monitoring Cyber Incidents in Cloud computing."
35. A banking corporation shall deploy to cope with cyber incidents in cloud-computing services in the following ways, among others:
    (a) cyber exercises;
    (b) cyber-incident scenarios including, at the very least:
        1. a situation in which the cloud-computing service may remain active and accessible but the reliability of the data that it shows cannot be trusted;
        2. attacks on the backup system of the cloud-computing service;
        3. attacks that require, as part of handling with them, cessation of access from specific destinations.
    (c) the performance of at least one representative worst case scenario of one or more activities in its material cloud-computing services.

36. A banking corporation must make sure that information-security and cyber-defense means are in place for all access channels to and from the cloud-computing service, making it possible to minimize the use of these channels to attack the banking corporation.

Chapter G2: Business Continuity

37. Insofar as cloud computing is a critical service for the banking corporation, the relevant requirements in Proper Conduct of Banking Business Directive 355, "Business Continuity Management," shall apply to it.
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 the foreign country. The banking corporation shall also assess the service provider's ability to maintain business continuation amid local attribution threats of the host country.
39. At a main or alternate cloud-computing site, a banking corporation must make sure 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

40. 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."

Updates

Circular no.	Version	Details	Date
2536	1	Original Supervisor's Letter	July 5, 2017
2579	2	Revision	November 13, 2018
2669	3	Revision	September 30, 2021

2715	4	Revision	June 13, 2022

Appendix A—Examples of Material Cloud computing—Cancelled

Appendix B—Main Aspects of Cloud-Computing Risk Assessment

(a) Regulatory risk originating in use of a cloud located outside the borders of the State of Israel—difficulty in complying with laws and regulations of the State of Israel and of the country where the service or the data operate or stored. Due to differences in legislation between countries, It is important to relate, *inter alia*, to issues such as the provider's duty to share information with legal and law-enforcement entities even without the banking corporation's knowledge, as well as to aspects of privacy protection.

(b) Risk originating in the use or non-use of a multi-cloud configuration (cloud infrastructures based on a combination of several different cloud-computing solutions).

(c) The data lifecycle, including location, proliferation of copies, and disclosure of data.

(d) Data, components, and systems portability—For example, does the use of a given cloud-computer service provider's cloud components limit the banking corporation and possibly deprive it of the ability to switch cloud-computing service providers or transfer information or systems back to bank premises.

(e) Information security and cyber defense risks, including information leakage, use of dedicated security tools, the manner of managing encryption keys, cloud-computing service that provides information security and cyber defense measures as the sole layer of defense.

(f) Access authorizations using appropriate tools for a cloud-computing environment.

(g) Change Management (CM) and Information Technology Assets Management (ITAM), including attention to the need to have the cloud-computing service provider to make changes as the result of technogical developments and changes in the services delivered, the banking corporation's control of changes in the systems, and the compatibility of the processes of change with the banking corporation's policies and procedures.

(h) Business-continuity and BCP/DRP risks, including changes in the banking corporation's Network Configuration and the geographical location of the cloud servers and including backup servers.

(i) Risks related to Workspace and management tools that may make system operation more complex.

(j) Legal risks, including aspects of confidentiality, data retention and retrieval, ownership of information, and licensing of softwares.

(k) Ongoing operational risks (including support personnel, working processes, incidents management, etc.), handling of irregular incidents, and mitigation of such risks by means including reporting and handling arrangements and settling responsibilities between the banking corporation and the cloud-computing service provider.

(l) Risks related to the attack surface, such as the integration of mobile devices (mobile phones, tablets, and other) into the cloud-computing service.

(m) Cloud-computing service supply-chain risks.

(n) Maintaining logical and administrative separation of different customers' systems in the cloud.

Appendix C—Monitoring Cyber Incidents in Cloud computing

(a) Monitoring of cloud activity shall be integrated into the banking corporation's current monitoring array. The management and definition of monitoring shall be undertaken by the banking corporation such that said management shall be at least commensurate with the nature of implementation in the cloud.

(b) In accordance with the provisions of Section (a), monitoring shall include, *inter alia,* deviations from legitimate activity in the banking corporation's infrastructure that are associated with cloud-computing services, e.g., changes in network architecture (segmentation), installation of a new server, access to databases, changes in encryption mechanisms, and aberrant network traffic in the cloud environment.

(c) If said monitoring is implemented by means of tools provided by the cloud-computing service provider, it should be ascertained that the tools meet accepted standards and are integrable into the existing monitoring systems of the banking corporation.

(d) Insofar as the banking corporation uses a monitoring system positioned in cloud environments within the same infrastructural environment in which a material cloud-computing service of the banking corporation exists, the banking corporation shall specify control operations for the continued continuity of monitoring of the material cloud-computing service at such time as communication between the banking corporation and the monitoring system of the cloud environment is disrupted.