Bank of Israel
Banking Supervision Department
Policy and Regulation Division

April 24, 2018
Circular no. C-06-2560

Attn:
Banking corporations and credit-card companies

Re: Supply Chain Cyber Risk Management
(Proper Conduct of Banking Business Directive no. 363)

General remarks

1. Financial organizations around the world and in Israel have been experiencing a growing number of cyber incidents in recent years. Most events of these types are characterized, among other things, by massive damage and sophisticated and innovative methods of attack, sometimes originating in external parties that provide banking corporations with various services. These entities are included in the banking corporations' supply chain. Accordingly, banking corporations must determine the actions that they should take to make sure that external material service providers do what is necessary to mitigate the banking corporation's exposure to cyber-risks.

2. The purpose of this Directive, "Supply Chain Cyber Risk Management," is to clarify the banking corporation's responsibilities for maintaining a secure working environment vis-à-vis external material service providers and its commitments to adequate cyber-risk management in these service providers' activity on the providers' premises, on the corporation's premises, and in providers' interfaces with the corporation.

3. When a material service provider is a corporate member of the banking group (e.g., a bank, a credit-card company, etc.), the requirements in this Directive may be implemented in accordance with the banking corporation's risk assessment.

4. The Banking Supervision Department is drafting a far-reaching directive on the topic of outsourcing. In the future, this directive will be inserted into it.

5. After consulting with the Advisory Committee on Banking Matters and with the approval of the Governor, I have established this Proper Conduct of Banking Business Directive, as specified below.

Structure of the Directive

6. The Directive comprises four chapters:

   (a) Chapter A: Background—including Introduction and Incidence;

   (b) Chapter B: General Remarks—specification of general provisions;

(c) Chapter C: Contracting—provisions relating to the framework of banking corporations' contracts with material service providers;

(d) Chapter D: Support and Maintenance—activities that entail strong authentication measures and security and control mechanisms in regard to remote access by a material service provider.

Introduction and Incidence (Sections 1–7 of the Directive)

7. The Directive relates to "material service providers": external parties that are included in the banking corporation's supply chain (such as companies that support capital-market trading services) that are material to the corporation's activity and/or expose the corporation to potentially acute cyber and information-security risks that, if they come to pass, make it possible to attack the banking corporation or impair its activity. The references is to external parties that provide the corporation with information-technology services such as support and/or maintenance of information systems, storage of sensitive data off the corporation's premises, technological outsourcing services, and the like. Providers of catering services, janitorial services, energy, and so on, are not at issue.

8. The purpose of the Directive is to describe the actions that banking corporations should take in managing cyber and information-security risks that derive from services delivered by material service providers.

General Remarks (Sections 8–11 of the Directive)

9. The Directive requires banking corporations to lay down principles governing the undertakings of material service providers in regard to cyber-risk management and to ensure that said providers comply with these principles. In addition, contracts with material service providers should make specific reference to this matter.

10. Banking corporations must perform a periodic mapping of their material service providers and review their contracts, material service providers' compliance with their undertakings, and the need to update contracts as a result of changes in services that the provider delivers and technological changes that affect the risk assessment. The purpose of said review is to allow the banking corporation to assess the risks deriving from the services delivered by the material service providers. If relevant players in the banking corporation reach the conclusion that the material service provider is exposing the corporation to significant cyber risks (e.g., when the service provider fails to meet certain undertakings or meets them inadequately), they must report this to the corporation's management. The bank's risk-management function should participate in the risk assessment in order to tender its opinion on the severity and implications of these risks. On the basis of said report and risk assessment, management should weigh and decide about the continuation of its contract with the material service provider (e.g., cutting back on activity, introducing compensatory controls at the banking corporation, terminating the contractual relationship, etc.).

11. Notably, Sections 10 and 11 apply to material service providers with which contracts are concluded before the Directive goes into effect. In any case, banking corporations shall examine and manage the risks inhering to existing

contractual relations with material service providers and shall, accordingly, consider the way in which the contractual relationship should continue to exist.

Contracting (Section 12 of the Directive)

12. When they contract with an material service provider, banking corporations must take account of the need to include in the contract the aspects specified in Section 12 of the Directive, and this, in accordance with the assessment of the risks deriving from the service and/or the activity, with emphasis on the following:

    (a) Section 12(a) of the Directive—we emphasize that the intent of the instruction is to strengthen systems owned by the material service provider that are installed on the premises of the banking corporation (and not on those of the service provider).

    (b) Section 12(e) of the Directive—subjecting employees of the material service provider who are involved in the provider's activity with and/or service for the banking corporation, and in accordance with the assessment of the risks deriving from the activity and/or the service, to reliability checks.

    (c) Section 12(f) of the Directive—appointing an information-security and cyber trustee at the service provider: this person may be chosen from among the service provider's employees.

    (d) Section 12(g) of the Directive—We emphasize that this does not mean presenting a list of all third-party (secondary) service providers of the material provider, but rather third-party service providers who support services that the material provider delivers to the banking corporation. Also, banking corporations are expected to update, as necessary, their assessment of the risks inhering to the service delivered by the material service provider after they receive said list of third-party providers, e.g., when a third-party provider stores sensitive data of the banking corporation on a public cloud.

    (e) Section 12(h) of the Directive—The section pertains to the creation of arrangements for the deletion of a banking corporation's data that are kept on the premises of the material service provider at the end of the contractual relationship between the parties, or at the request of the banking corporation at any time proceeding the end of the relationship, e.g., in the event of concern about leaking of information and/or other cyber event.

    Section 12 of the Directive means that the corporation shall use discretion, on the basis of the risk assessment, about whether these instructions should be anchored in its contract with the service provider. A situation in which the corporation has no way of inserting a certain instruction into the contract despite the risk attending to it shall be taken into account in respect of the risk assessment set forth in Section 10 of the Directive.

Support and Maintenance (Sections 13–14 of the Directive)

13. In accordance with the risk assessment, banking corporations shall specify activities for which material service providers must satisfy strong authentication requirements. This refers to service-provider activities that may expose the banking corporation to acute risk, such as maintenance of the banking corporation's systems or remote access.

14. In regard to remote access, in view of the risks that inhere to this activity, the banking corporation, in accordance with the risk assessment, shall have security and control mechanisms in place that will help to mitigate them, as specified in Chapter D of the Directive.

Date of Effect and Transitional Provisions

15. This Directive shall go into effect no later than six months after it is gazetted the (hereinafter: the date of effect).

16. Notwithstanding the contents of Section 15 *supra*, banking corporations shall begin to carry out the processes specified in Section 10 of the Directive from the date on which the Directive is gazetted.

17. The Directive shall apply to contracts that are concluded with service providers (including renewal of contracts) **after** the date of effect.

18. In regard to contracts with service providers that are concluded (or renewed) **before** the date of effect—the next time the contract is up for renewal and no later than nine months after the Directive is gazetted, banking corporations shall act in accordance with Section 10 of the Directive and their management shall weigh and decide on whether to continue the contractual relationship with the material service provider, the need to update the existing contract, and the date by which said update should be carried out.

Revised file

19. Update pages for the Proper Conduct of Banking Business Directive file are attached. Following are the provisions of the update:

Remove page	Insert page
———	(4/18) [1] 363-1-5

Respectfully,

Dr. Hedva Ber

Supervisor of Banks

Supply Chain Cyber Risk Management

A. Background

Introduction

1. Financial organizations around the world and in Israel have been experiencing a growing number of cyber incidents in recent years. Most of the cyber incidents are characterized, among other things, by massive damage and sophisticated and innovative methods of attack, sometimes originating in external parties that provide various services to the banking corporations . These entities are included in the banking corporations' supply chain.

2. Proper Conduct of Banking Business Directive 361, "Cyber Defense Management," expresses the need to have in place an effective process for risk detection and assessment, *inter alia* with regard to banking corporations' external activity environments and their work with external service providers. The directive also states that supply-chain management and dependency on external entities processes, shall be included in the cyber defense array. In addition, the directive requires a banking corporation to have necessary processes in place with which to ascertain that external entities are taking the necessary measures to mitigate the banking corporation's exposure to cyber risks.

3. It should be emphasized that some external entities that belong to a banking corporation's supply chain (such as companies that support capital-market trading services) are material to its activity and/or expose it to potentially high cyber and information-security risks that, when they eventuate, make it possible to attack the banking corporation or impair its activity (hereinafter: material service providers).

4. The purpose of this directive is to clarify the banking corporation's responsibility for maintaining a secure working environment vis-à-vis material service providers and it's obligation to manage the cyber-risks appropriately in regard to these service providers' activity on their own premises, on the banking corporation's premises, and in material providers' interfaces with the corporation.

5. Notwithstanding the contents of Section 3 *supra*, when the material service provider is a corporate member of the banking group, the requirements in this directive shall be implemented in accordance with the banking corporation's risk assessment. For the purposes of this section, a "banking group" is a banking corporation, a banking corporation that controls it, and corporations controlled by either of them.

6. The Banking Supervision Department is drafting a far-reaching directive on the topic of outsourcing. In the future, this directive will be inserted into it.

Incidence

7. (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) an acquirer as defined in Section 36i.

(b) The Supervisor may issue specific provisions, other than those set forth below, that shall apply to a specific banking corporation or, in exceptional cases, may absolve a banking corporation from a specific instruction specified below.

B. General Remarks

8. Banking corporation shall lay down principles for the obligations of material service providers toward it in respect of cyber risk management.

9. In its contract with a material service provider, a banking corporation shall define specific reference to the management of cyber risks (see Chapter C below) and shall ensure that the provider abide by the principles that the banking corporation has established (Section 8 *supra*).

10. A banking corporation shall conduct the following on a periodic basis:

    (a) mapping of its material service providers; examination of the contract with them; compliance with their contractual undertakings; with reference to the need to make necessary changes on the supplier's part pursuant to developments and technological changes and changes in services rendered.

    (b) a risk assessement derived from the services provided by the material service providers, also based on the examination referenced in Section 10(a) *supra* and the results of the overviews specified in Section 12(c) below.

11. In the event that relevant players in the banking corporation reach the conclusion, after the examination referenced in Section 10 *supra*, that a material service provider does not meet its obligations in a manner that exposes the banking corporation to significant events, they shall report this to the corporation's management, describing said risks and their implications on the corporation and its customers. In this case, management shall consider and make a decision on continuing to contract with the provider.

C. Contracting

12. When it contracts with a material service provider, a banking corporation shall take into account the need to include the following in the contract, in accordance with the risk assessment:

(a) hardening systems of the material service provider that are installed on the banking corporation's network in accordance with the banking corporation's information-security and risk-management procedures.

(b) transferring log files from the service provider's systems, at the banking corporation's request.

(c) producing an overview of a Vulnerabilities Survey and controlled Penetration Tests on a periodic basis, at the request of the banking corporation, including the test scenarios, and in accordance with risk management.

(d) dealing with findings detected in the Survey and the Penetration Tests within a reasonable time after their discovery.

(e) subjecting employees of the material service provider who are associated with service given to the banking corporation to reliability checks.

(f) appointing an information-security and cyber trustee with the material service provider and defining his/her powers and duties.

(g) providing a list of third-party (secondary) service providers who support the services that the material service provider gives to the banking corporation, on a periodic basis that the banking corporation shall determine.

(h) making arrangements for the deletion of banking-corporation data that are stored on the service provider's premises after the end of the contractual relationship and/or at the request of the banking corporation.

(i) creating a separation of working environments (development, production, etc.) on the material service provider's premises.

(j) reporting to the banking corporation about cyber incidents that occur at the material service provider or its third-party providers.

D. Support and Maintenance

13. Banking corporations shall specify activities, in accordance with the risk assessment, for which the material service provider shall have to use strong authentication (2FA) in matters such as remote access to the banking corporation's systems, maintenance of the corporation's systems, and so on.

14. Banking corporations shall establish remote-access security and control mechanisms vis-à-vis the material service provider, in accordance with the risk assessment, such as denying access except with the corporation's approval; secured access from an activity environment separate from the material service provider's other working environments; operating a timeout mechanism after an interval in which the material service provider conducts no activity; recording and monitoring of maintenance activity; and so on. In addition, access to the banking corporation's production environment should not be allowed unless the corporation approves it.

Updates

Circular no.	Version	Details	Date
2560	1	Original circular	April 24, 2018