BANK OF ISRAEL Banking Supervision Department Technology, Innovation, and Cyber Division Banking Technology Unit	

Jerusalem

June 17, 2026

Circular No. C-06-2848

To: The Banking Corporations and Payment Service Providers with Prudential Importance License Holders

Re: Reporting of Technology Failure Incidents, Information Security Incidents, and Cyber Attacks
(Proper Conduct of Banking Business Directive No. 366)

Introduction

1. On 18 November 2024, the Banking Supervision Department issued Proper Conduct of Banking Business Directive No. 364, "Management of IT, Information Security, and Cyber Defense Risks" (hereinafter: "Directive 364"). In accordance with Circular 06 No. 2799 (hereinafter: "the Circular") accompanying the publication of the Directive, Directive 364 entered into force on May 18, 2026.
2. Section 8 of the Circular stated that: "…in order to create consistency in the use of the terminology established in this Directive[1] throughout the existing regulatory framework relating to information technology, the Banking Supervision Department intends to publish amendments to the relevant directives, including Proper Conduct of Banking Business Directive No. 366, 'Reporting of Technology Failure and Cyber Incidents'…" The current update incorporates, among other things, the required adjustments referred to above.
3. In addition, the Directive has been updated based on lessons learned and insights gained by the Banking Supervision Department from its review of work processes implemented by various banking corporations in preparation for technology failure and information security incidents, as well as from practical experience with the implementation of the Directive during actual occurrences of such events.
4. This regulatory amendment was not accompanied by a report under the Regulatory Principles Law, 5782-2021 (hereinafter in this section: "the Law"),

[1] Proper Conduct of Banking Business Directive no. 364 on "Management of IT, Information Security, and Cyber Defense Risks".

pursuant to Section 34(c)(2) of the Law, as the direct and indirect impacts expected to result from the regulation on the entities to which it applies, including compliance costs, are not considered material.

The regulation will be subject to an ex post review under Section 36 of the Law, ten years after its effective date.

5. Following consultation with the Advisory Committee on Banking Business Affairs and with the approval of the Governor, I have decided to update Proper Conduct of Banking Business Directive No. 366, "Reporting of Technology Failure and Cyber Incidents."

Amendments to the Directive

6. **Introduction**

Section 1

Adjustments were made to clarify the relationship between this Directive and Directive 364.

7. **Applicability**

Section 3

The application section has been amended so that entities defined in Sections 11(a)(3a), 11(a)(3b), and 11(b)(2) of the Banking (Licensing) Law, 5741-1981 (hereinafter: "the Banking (Licensing) Law") are no longer generally subject to the reporting requirements of this Directive.

Accordingly, these entities are now required to report to the Banking Supervision Department only in the event of technology failure incidents or information security incidents, including cyberattacks (hereinafter: "an Incident"), as required under Section 6.5 of the Directive. That is, given the relatively limited impact of such entities on the banking system, only incidents that would otherwise be reportable under Sections 6.1-6.4 of the Directive and that have a material impact, including technological, reputational, or financial implications for the controlling banking corporation, the banking group, or the banking system, must be reported to the Banking Supervision Department. Incidents whose impact is limited solely to the entity itself are not required to be reported.

In addition, the section has been updated to align with the current wording of the Banking (Licensing) Law. The term "acquirer", as previously defined in Section 36i of the Law, has been replaced by "Payment Service Provider with Prudential Importance License Holder", as defined in Section 36i of the Law. For the avoidance of doubt, Section 6.5 of the Directive also applies to subsidiaries of a Payment Service Provider with Prudential Importance License Holder.

8. Definitions

Section 5

The definition of "Significant Technology Failure Incident" has been expanded to emphasize that disruption to a business activity, process, or function includes disruptions that have a severe and widespread internal impact on the banking corporation, even where customers or the banking system are not directly affected.

Examples include:

- An outage in production systems operating in an active-active configuration, where the backup systems were activated and service continuity was maintained.
- A severe malfunction that was detected and remediated before any actual impact materialized reflecting technological risk potential, as distinct from information security or cyber incident potential.

Furthermore, to ensure regulatory consistency with Directive 364, which serves as the foundational framework for supervisory directives concerning information technology:

- The definition of "Technology Failure Incident" has been moved to Directive 364, and this Directive now references that definition.
- The terms "Information Security Incident," "Data Leakage," "Information Technology Array, Information Technology (IT)" "Cyber attack," "Damage," and "Third Party" are now defined by reference to their respective definitions in Directive 364.

9. Types of Incidents that Require Reporting

Sections 6 and 6A

The categories of incidents requiring reporting to the Banking Supervision Department have been clarified and expanded:

- Section 6.2 previously required reporting of incidents handled at the level of the Chief Cyber Defense and Information Security Officer (CISO). The requirement has now been clarified to specify that reporting applies to incident described in Section 6.2 that is managed by, or involves the participation of, the banking corporation's Chief Cyber Defense and Information Security Officer or another management function acting on his behalf.
- The reporting obligation, as well as the Directive's other provisions, will also apply where there is a concern regarding the occurrence of an information security incident with systemic implications, following a request by the Banking Supervision Department.

10. Responsibility for Reporting

Section 8

Adjustments have been made to ensure consistency with the terminology established in Directive 364, as described in Section 2 above.

Section 9

The section has been updated to reflect the change in the name of the division within the Banking Supervision Department responsible for information technology matters.

11. Manner of reporting

Sections 10 and 12

Adjustments have been made to reflect changes in:

- The name of the division within the Banking Supervision Department responsible for information technology matters; and
- The name of the unit within that division responsible for regulation and supervision of information technology in banking corporations.

Section 11

Adjustments have been made to ensure consistent use of the terminology established in Directive 364, as described in Section 2 above.

12. Investigation of the incident and Reporting

Section 14

To maintain the quality of incident investigations and to ensure that lessons learned and actionable insights can be derived to improve preparedness and potentially prevent similar incidents in the future, a new requirement has been added stipulating that investigations must be conducted by, or at least with the involvement of, a party that was independent of the incident.

Section 15

A clarification has been added stating that any incident requiring reporting to the Banking Supervision Department under Section 6 of the Directive must also be subject to an incident investigation in accordance with this section.

13. Documentation of Incidents Not Reported

Section 17

Incidents for which a banking corporation assessed the need for reporting under this Directive and concluded that reporting was not required must be documented.

Such documentation must include:

- The person or function responsible for the decision; and
- The rationale supporting the decision.

This documentation will serve as evidence for supervisory reviews or examinations relating to the banking corporation’s exercise of judgment regarding reporting obligations under this Directive.

Effective Date

The amendments to the Directive shall take effect on the date of publication of this Circular.

Update to the Proper Conduct of Banking Business File

Attached are the update pages for the Proper Conduct of Banking Business compilation, as follows:

Remove pages	Insert pages
(01/23) [4] 366-1-4	(06/26) [5] 366-1-5

Sincerely,

Daniel Hahiashvili
Supervisor of Banks
Bank of Israel