Reporting of Technological Failures and Cyber Events

Introduction and goals

1. The banks are an important layer in the everyday operations of the financial sector in Israel. Since the banks' information technology systems constitute a critical infrastructure for their business activity, the banks need to identify and deal with technological failures and cyber events as quickly and efficiently as possible, while at the same time continuing to operate and provide essential services. Accordingly, the bank's policy and its procedures for handling events of this type must relate to, among other things, the process for reporting to the Banking Supervision Department.
2. There are a number of goals for the reporting of technological failures and cyber events to the Banking Supervision Department:
   2.1 To ensure that the bank in which the event has occurred is managing the event in an optimal manner and to assist in the handling of the event if necessary.
   2.2 To enhance the ability to provide an up-to-date assessment of the situation in order to facilitate an informed decision as to whether the Banking Supervision Department should take any action and if so which action.
   2.3 To identify the potential for a systemic event and to limit the effect of the event on other banks to whatever extent possible.
   2.4 To identify the areas in which the bank or the banking system as a whole needs to adopt measures in order to prevent the reoccurrence of events of this type or measures that will improve the resilience of the banks to events of this type in the future.
   2.5 To enable the Banking Supervision Department to prepare for similar scenarios in the future based on appropriate assessment of risk to the banking system.
   2.6 To ensure that the event is investigated and conclusions drawn.

Applicability

3. (a) This directive will apply to the following banks as defined in the Banking (Licensing) Law, 5741 – 1981 (herein: a "bank"):
   (1) A banking corporation;
   (2) A corporation as defined in Sections 11(a)(3a) and (3b);
   (3) A corporation as defined in Section 11(b);
   (4) A clearinghouse as defined in Section 36i;

   (b) The Supervisor of Banks can issue directives that differ from the aforementioned and which will apply to a particular bank or can exempt a bank from a particular directive, in exceptional cases, under specific circumstances that he views as justifying the decision and for reasons that will be documented.

4. The reporting will apply to each bank separately, even if the event occurs simultaneously in a number of banks that belong to a single banking group.

Definitions

5. In this directive, the following terms will have the following definitions:

Technological failure event	An event, incident or result that is not expected or planned as part of the bank's normal activity and which has a disruptive effect on the normal activity of the bank's information technology system or on the services provided by it.
Significant technological failure	A technological failure that causes a disruption of business activity, of a process or of a function that has a severe and broad effect on the bank's activity, on the services it provides to its customers or on the banking system as a whole.
Cyber event	According to its definition in Proper Conduct of Banking Business 361 on "Cyber Defense Management".
Damage	According to its definition in Proper Conduct of Banking Business 361 on "Cyber Defense Management".
Event status	A description of the current stage of the reported event: Identification – identification of the event. Analysis – identification of the event's source and its scope. Halt of intensification / containment – Halt of event intensification. Treatment / eradication – implementation of measures to repair / neutralize the attack components found within the bank. Rectification / restoration – Return to fully normal activity.
Accepted working hours	The accepted working hours for the purposes **of this directive only**: Sunday to Thursday that are business days in the banking system, from 8:00 to 18:00.

Types of events that require reporting

6. Following are the types of events that require reporting to the Banking Supervision Department:
   6.1 A significant technological failure.
   6.2 A suspected cyber event that is dealt with at the level of the Cyber Protection Officer and whose handling was not completed within four hours from the time of its initial identification or within two hours from the point at which there was knowledge of damage that it had caused.

6.3 A cyber event that affects a large number of customers and/or has new offensive characteristics.

6.4 Any significant information leakage event that is not specified in Subsections 6.1 to 6.3.

Responsibility for reporting

7. A bank will decide on a member of the Executive whose responsibility it will be to fulfill the conditions of this directive.
8. Reporting Officer:
   8.1 A bank will appoint a Reporting Officer for Technological Failure and a Reporting Officer for Cyber Events.
   8.2 Every technological failure and/or cyber event as mentioned in Section 6 above will be reported to the Banking Supervision Department by the Reporting Officer appointed by the bank.
   8.3 The two functions mentioned in Subsection 8.1 above can be carried out by one officer, according to the decision of the bank.
   8.4 A permanent acting reporting officer can be appointed for each of the reporting functions.
9. A bank will submit the details of the officer according to Sections 7 and 8 above to the Technology and Innovation Branch of the Banking Supervision Department and will provide an update of any change in those appointments, including changes in their details.

Manner of reporting

10. **Initial reporting of the event –**
    10.1 A bank will submit a report by telephone within two hours of identifying the event as one that requires reporting according to Section 6 above and subsequently will supplement that with a written initial report within 8 hours from the time of the telephone report. The Banking Supervision Department can extend or shorten the aforementioned time limits for a written report if the circumstances justify that decision.
    10.2 The telephone report will be made at any time of day, regardless of the accepted working hours.
    10.3 The telephone report will be conveyed, according to the circumstances, to the Director of the Unit for Regulation and Auditing for Information Technology and/or the Director of the Supervisory Cyber Unit in the Technology and Innovation Branch of the Banking Supervision Department.
    10.4 If the time to make the initial written report is outside the accepted working hours, then it will be submitted at the start of accepted working hours on the following day.
11. A significant technological failure event will be reported as an event in which there is a suspicion that a cyber event has occurred (in the appropriate field on the reporting form) as long as it has not been proven that there is no such suspicion.

12. **Additional reports during the event –**
    12.1 A bank will be required to submit up-to-date information on the event in writing, on the last reporting form submitted as mentioned above, at least once daily or at any time that there are significant changes in the characteristics of the event and/or its consequences, included the criteria for reporting as described in Section 6. The Banking Supervision Department can approve a request from a bank to lessen the frequency of the reporting for a specific event, if the circumstances justify that decision. The aforementioned approval will be valid as long as there has been no significant change in the characteristics of the event or its consequences.
    12.2 Without detracting from what is stated in Subsection 12.1 above, it should be clear that an event that was reported on the basis of one of the criteria listed in Section 6 and for which it later becomes clear that additional criteria are fulfilled does not require an additional new report, but rather an update will be made regarding the additional criterion in subsequent reports.
    12.3 In the case that there is a significant development in an event for which there is already a reporting process going on, at a time outside regular working hours, then an update will be provided by telephone to the responsible official in the Technology and Innovation Branch within the Banking Supervision Department (as mentioned in Section 10.3 above) and subsequently a written report will be submitted, as required.
13. **Reporting the completion of an event –**
    13.1 A bank is required to report the completion of an event.
    13.2 The bank will verify that the form is complete and contains the most up-to-date information as of the time that the report on the completion of the event is submitted.

Investigation of the event

14. A bank will establish an event investigation procedure, which will specify among other things the method of investigation and the officials that will carry it out.
15. A bank will implement an investigation on the completion of the event according to the procedure it has established. The investigation will include at least the following items:
    15.1 Final and up-to-date details of the event and the circumstances of its occurrence (while relating to all of the details that were reported to the Banking Supervision Department).
    15.2 A final report, including recommendations, the installation of internal controls, a schedule for implementation, a list of the officials involved in the investigation and the official approving the investigation.
16. The investigation will be approved by the member of the Executive responsible for fulfilling this directive, as mentioned in Section 7 above, and it will be submitted to the Banking Supervision Department within 45 days from the completion of the event or within 60 days from the date on which the event was identified as an event

that requires reporting according to Section 6 above, according to the earlier of the two.

Updates

Circular 06 no.	Version	Details	Date
2643	1	Original circular	December 29, 2020