



Directive 17d

Risk Management at a Payment-System Operator

1.	Introduction	2
2.	Definitions	3
3.	Incidence	4
4.	Lines of defense in risk management at a payment-system operator	4
5.	Board of Directors and senior management responsibilities	5
6.	Chief Risk Officer	7
7.	Duties and frame of work of the risk-management function	8
8.	Independence and avoidance of conflict of interests	9
9.	Professional fitness	9
10.	Letter of appointment	10
11.	Risk-management policy and framework	10
12.	Risk appetite	11
13.	Risk detection, measurement, and evaluation	12
14.	Stress tests	13
15.	Monitoring and reporting risks	14
16.	Risks Document	14
17.	Incentives for risk management	15
18.	Recovery plan and orderly-liquidation plan	16
19.	Information reported and frequency of reportage	16
20.	Forwarding information to the Bank of Israel	17
21.	Promulgation and update of Directive	18



1. Introduction

In accordance with Section 8 of the Payment Systems Law, 5768-2008 (hereinafter: “the Payment Systems Law”), an operator of a controlled payment system shall formulate rules that will ensure the stability, efficiency, and sound functioning of the system and shall ensure the availability of measures with which to manage risks that exist or may exist in the system, prevent them, and ensure the existence of backup arrangements at the system in the event of an emergency.

In accordance with Principle 3 of the Principles for Financial Market Infrastructures (PFMI), published in 2012 by the Committee on Payment and Settlement Systems of the BIS (CPMI) and the International Organization of Securities Commissions (IOSCO), a financial-service infrastructure (FMI) should have in place a sound risk-management framework for comprehensive management of legal, credit, liquidity, operational, and other risks.

In accordance with Principle 2 of the Principles for Financial Market Infrastructures (PFMI), the Board of Directors and senior management should lay out a policy and framework for comprehensive risk management in order to detect, measure and evaluate, monitor, report on, and manage an FMI.

An effective and broad risk-management array, spanning the entire organization is a key fixture in assuring the long-term stability of a payment system.

This Directive lays down basic principles for risk-management and -control at controlled payment systems so that said systems they will be better able to detect and manage risks optimally, as reflected in the system’s activity and decision-making.



2. Definitions

“Risk management” —	Processes meant to detect, evaluate, and measure potential risks, analyze them, and take measures to prevent them and mitigate their impact;
“Risk appetite” —	the level of risk, in quantitative and qualitative terms, that the Board of Directors is interested in assuming;
“Risk capacity” —	the maximum risk that the payment system can absorb under various constraints and extreme scenarios;
“Risk profile” —	the aggregate level of risk embodied in payment-system activity at a specific point in time;
“Risk-management framework” —	a framework that includes risk-management policies, procedures, and controls;
“Risk foci” —	any individual exposure or group of exposures that may cause large losses or a material change in the risk profile of a payment-system operator;
“Chief Risk Officer”	The head of a payment-system operator’s risk-management function;
“Risk-management function”	an independent function tasked with managing a payment system’s risks as part of the second line of defense.



3. Incidence

- 3.1 This Directive shall apply to every payment-system operator that the Governor has declared a controlled payment system or a designated controlled payment system.
- 3.2 The Bank of Israel may, as circumstances shall indicate, establish certain instructions, different from those specified below, that shall apply to a certain payment-system operator, and may exempt a payment-system operator from the incidence of certain sections of this Directive.
- 3.3 In a payment-system operator that has no Board of Directors function due to its statutory, legal, or organizational structure, the obligations of a Board of Directors established in this Directive shall apply to the function that corresponds to a Board of Directors or the highest function that bears responsibility for the business and solidity of the payment-system operator.
- 3.4 In respect of systems that are run by the central bank, this Directive shall apply as tailored to the corporate-governance structure of the central bank.¹

4. Lines of defense in risk management at a payment-system operator

- 4.1 Appropriate corporate governance for risk management is based on three lines of defense:
 - 4.1.1 First line of defense—the managements of lines of business, including support functions, are responsible for detecting, evaluating, measuring, monitoring, mitigating, and reporting structural risks in products, activities, processes, and systems for which they are responsible, and for managing an appropriate control environment in the context of risk management;

¹ In this context, in August 2015 the BIS published a document titled “Application of the Principles for Financial Market Infrastructures to Central Bank FMIs,” with guidelines as to how the PFMI rules should be applied to payment systems run by a central bank.



- 4.1.2 Second line of defense—an independent risk-management function, tasked with complementing the risk-management activities of the line of business that uses the first line of defense;
- 4.1.3 Third line of defense—the internal-audit function, which carries out independent review and challenges the risk-management controls, processes, and systems of the payment-system operator.

5. Board of Directors and senior management responsibilities

- 5.1 Every payment-system operator shall establish a permanent risk-management function.
- 5.2 The Board of Directors and senior management shall ascertain that the stances of the risk-management function will play an important role of the array of considerations in making business decisions.
- 5.3 **The Board of Directors of a payment-system operator is responsible for:**
 - 5.3.1 ascertaining the existence of an effective risk-management function that carries out and oversees its duties independently;
 - 5.3.2 appointing a Board of Directors risk-management committee;
 - 5.3.3 ascertaining that the Chief Risk Officer has the deserving status and the necessary resources for the discharge of her or his duties;
 - 5.3.4 establishing clear risk-management policies and a comprehensive risk strategy, including risk appetite, risk capacity, and a risk-management framework;
 - 5.3.5 discussing and approving, at least once per year, the risk appetite and the risk-management framework enshrined in a policy document;
 - 5.3.6 tracking senior management's actions and ascertaining that the risk profile is consistent with the risk appetite laid down, in view of developments and changes in the financial markets and the external surroundings of the payment-system operator's risk-management practices and activities;
 - 5.3.7 deciding which matters to hand to the risk-management committee for thorough review.



5.4 The Board of Directors risk-management committee is responsible for:

- 5.4.1 advising the Board of Directors on comprehensive risk strategy, including current and future risk appetite and overseeing the way senior management applies said strategy and practice;
- 5.4.2 maintaining ongoing relations with the Chief Risk Officer;
- 5.4.3 reviewing risk-management activity and discussing the risk document at least once per year and whenever the risk profile undergoes a material change;
- 5.4.4 discussing, once per year, the results of stress tests and forward-looking scenario analyses that examine the payment-system operator's ability to stay within the risk-appetite limits established under a range of circumstances.

5.5 Senior management of a payment-system operator is responsible for:

- 5.5.1 effective management of the payment system's risks;
- 5.5.2 formulating, assimilating, and implementing a risk-management framework on the basis of the risk appetite laid down by the Board of Directors;
- 5.5.3 ensuring that the payment-system activities are consistent with the risk appetite and policies approved by the Board of Directors and does not deviate from the risk capacity even in extreme scenarios;
- 5.5.4 appointing a Chief Risk Officer and placing him or her in charge of the risk-management function and applying the risk-management framework in practice;
- 5.5.5 ascertaining the existence of adequate resources for risk-management at the payment-system operator, including suitably experienced and qualified staff, access to resources, and adequate information systems;
- 5.5.6 ascertaining that the first line of defense assumes initial responsibility for risk management;
- 5.5.7 promoting the assimilation of a risk-management culture at the organization level;
- 5.5.8 establishing procedures for reporting on and learning from events;



-
- 5.5.9 ascertaining that the risk profile does not deviate from the risk appetite; when examining a new product / service / system, too, it shall be ascertained that the new risks do not affect the risk profile in a way that would deviate from the risk appetite established.

6. Chief Risk Officer

- 6.1 The risk-management function shall be headed by the Chief Risk Officer.
- 6.2 The Chief Risk Officer shall be explicitly responsible for the risk-management function and the organization-level comprehensive risk-management framework.
- 6.3 The Chief Risk Officer shall be an employee of the payment system who has the status of a member of senior management and is directly subordinate to the Chief Executive Officer.
- 6.4 The Chief Risk Officer shall report directly to the Board of Directors by means of a risk-management committee.
- 6.5 The Chief Risk Officer shall be independent and shall have no additional responsibilities in regard to lines of business, income-generating functions, and additional staff or control duties that may be detrimental to his or her position.
- 6.6 The Chief Risk Officer shall be responsible for the following actions, *inter alia*:
- 6.6.1 compiling, once per year, the Risks Document of the payment system and presenting it to the Board of Directors or to the risk-management committee of the Board of Directors;
 - 6.6.2 discussing key risk-related issues with the Chief Executive Officer and the Board of Directors and emphasizing risk-management issues for their attention, including risk foci or situations in which the risk appetite established may have been breached;
 - 6.6.3 drawing up an annual work plan for the organization's risk-management array;
 - 6.6.4 validating, from time to time, the risk detection, measurement, and evaluation tools and methods.



-
- 6.7 The service of the Chief Risk Officer shall not be terminated, and the Officer shall not be removed from his or her position, for any reason whatsoever, except with the prior approval of the Board of Directors.

7. Duties and frame of the risk-management function's work

- 7.1 The risk-management function is responsible for helping senior management provide effective management of the risks that the payment system faces and for aligning the risk profile with the risk appetite established by the Board of Directors.
- 7.2 The work of the risk-management function shall include all constituents of the payment system.
- 7.3 The risk-management function shall ensure that all risks to which the payment system is exposed are managed appropriately by the relevant units and are presented to the Board of Directors from a comprehensive perspective.
- 7.4 The duties of the risk-management function shall include the following, *inter alia*:
- 7.4.1 assessing possible ways of managing risk exposures and recommending, where necessary, risk mitigation or hedging in order to limit exposure;
 - 7.4.2 encouraging senior management and lines of business to detect and evaluate risks in a critical manner that is not based on overly optimistic assumptions.
- 7.5 The risk-management function shall be involved in the following processes, at the very least, and shall receive prior reportage in time to enable it to evaluate and relate in writing to the risks inherent in them:
- 7.5.1 planning risk strategy, including determining risk appetite;
 - 7.5.2 constructing and updating a comprehensive risk-management framework;
 - 7.5.3 approving new products and areas of activity;
 - 7.5.4 amending the statutes;
 - 7.5.5 approving and validating risk-measurement and -evaluation systems, including models and stress tests;
 - 7.5.6 estimating risks that may materialize in mergers and acquisitions;



- 7.5.7 material organizational changes;
 - 7.5.8 approving major transactions with related parties and transactions that may have a major impact on the business results of the payment-system operator;
 - 7.5.9 complex legal processes.
- 7.6 The system operator shall ascertain that the stances of the risk-management function play an important role in the considerations behind decision-making in regard to the aforementioned processes.

8. Independence and avoidance of conflict of interests

- 8.1 The risk-management function shall be independent of the various lines of business.
- 8.2 The Chief Risk Officer and the risk-management function staff shall have no additional duties that create, or may create, a conflict of interest with their duties at the risk-management function.
- 8.3 Remuneration of risk-management function staff shall be consistent with the objectives of the function and shall not be made contingent on the performance of lines of business except under a general remuneration policy that applies to all payment-system staff.

9. Professional qualifications

- 9.1 The Chief Risk Officer and the risk-management function staff shall have adequate knowledge, expertise, experience, and training, including command of the field of risks and areas of activity of the payment system, to challenge lines of business in all aspects of risk that originate in their activity.
- 9.2 The professional qualifications of function staff shall be preserved and enhanced by means of training and professional development programs.



10. Letter of appointment

- 10.1 A letter of appointment for the Chief Risk Officer shall be drawn up.
- 10.2 Said letter of appointment shall relate to the following matters at the very least:
 - 10.2.1 the Chief Risk Officer's duties and the extent of his or her activity;
 - 10.2.2 the Chief Risk Officer's status, powers, and responsibilities in the organization;
 - 10.2.3 establishing a mechanism for cooperation and reportage between the risk-management function and functions on the first line of defense, other functions on the second line of defense, and the internal-audit function on the third line of defense.
- 10.3 The letter of appointment shall ensure the right and the authority of the risk-management function and the Chief Risk Officer:
 - 10.3.1 to enjoy access to lines of business so that they may understand business activity and gain access to crucial information;
 - 10.3.2 to enjoy unfettered and direct access to the payment-system operator's records, information, and information systems, subject to the provisions of the law.

11. Risk-management policy and framework

- 11.1 The risk-management framework shall be consistent with the risk appetite and shall relate to the totality of relevant material risks, including credit and liquidity risks and operational, business, general, and legal risks.
- 11.2 The risk-management framework shall be anchored in clear procedures that will ensure the following in respect of risk-management processes:
 - 11.2.1 efficient and effective management;
 - 11.2.2 the reliability, integrity, and timeliness of financial and managerial information;
 - 11.2.3 compliance with the payment-system operator's various obligations, including those flowing from statutes and regulations.



-
- 11.3 The risk-management framework shall be anchored in a policy document that specifies the risk appetite and the way each material risk shall be managed.
- 11.4 Said policy document shall include the following, *inter alia*:
- 11.4.1 standardization of risk terminology in order to ensure consistency in risk detection, ranking of exposures, and risk-management goals;
 - 11.4.2 description of the structure of risk-management governance and clear separation of the three lines of defense;
 - 11.4.3 lines of reportage and accountability;
 - 11.4.4 description of methodologies and tools for risk detection, measurement, evaluation, and monitoring, and their use.
- 11.5 Said policy document shall be reviewed at least once per year and updated commensurate with developments and changes in the payment-system operator's external operating environment, strategy, products, activities, and systems.
- 11.6 The risk-management framework shall serve as a basis for detection, management and evaluation, monitoring, reporting, and management of the payment-system operator's risks and shall relate to routine and non-routine matters including potential inability of participants and the payment system to meet their obligations.

12. Risk appetite

- 12.1 The payment-system operator shall produce a comprehensive system-level risk-appetite document that the Board of Directors shall approve once per year.
- 12.2 In defining the risk appetite, the following shall be taken into account:
- 12.2.1 all material risks;
 - 12.2.2 constraints on capital and sources of funding;
 - 12.2.3 obligations of payment system;
 - 12.2.4 impact of potential extreme events;
 - 12.2.5 a range of quantitative indicators, well defined and including the information that is needed to understand the risk appetite;



12.2.6 qualitative components for each risk and at the overall corporation level, such as strategic directions and desirable business restraints, undesirable activities from the standpoint of the payment-system operator, and basic principles of the risk-management framework.

12.3 Any revision of the risk appetite shall be approved by the Board of Directors in an orderly and documented proceeding, including a detailed account of the rationale behind said revision.

13. Risk detection, measurement, and evaluation

13.1 The payment-system operator shall use methods and tools to detect, measure, and evaluate risks, basing itself, *inter alia*, on the following guidelines:

13.1.1 use of quantitative and qualitative components;

13.1.2 avoidance of overreliance on any specific risk-measurement method and, where possible, use of a variety of measurement tools or methods, including expert evaluation, in order to examine the exposure from different points of view;

13.1.3 covering a range of scenarios without relying on overoptimistic assumptions about dependency ratios and correlations;

13.1.4 avoidance of overreliance on outside risk assessments;

13.1.5 review of performance relative to risk assessments in accordance with outcomes, evaluating the precision and effectiveness of the risk-management process and adjusting measurement methods and models where necessary;

13.1.6 The payment-system operator shall act to detect and analyze risk foci originating in risks that share similar elements. For this purpose, the operator shall account for similar exposures, including those in different lines of business, that cross different statutory entities, types of assets, areas of risk, and geographic regions.

13.2 Risk detection shall be carried out for the following, *inter alia*:



-
- 13.2.1 all risks that inhere to the payment system, risks to which the payment system is directly exposed by its participants, customers, and other entities, and risks to which the payment system directly exposes them;
 - 13.2.2 all critical risks that may materially impair the ability of the payment system to continue meeting its obligations and/or operate as a going concern;
 - 13.2.3 risks that do not seem material and/or relevant in themselves but deserve attention if combined with other risks;
 - 13.2.4 risks that may be interrelated and that may interact;
 - 13.2.5 risks associated with activity of the payment-system operator other than clearing and settlement activity, if relevant, and examining whether these risks are also affecting core activity.

14. Stress tests

- 14.1 A payment-system operator shall use forward-looking stress tests.
- 14.2 Said stress tests shall assist the payment system in the following processes:
 - 14.2.1 capital and liquidity planning;
 - 14.2.2 reviewing risk appetite;
 - 14.2.3 detecting existing or potential risk foci;
 - 14.2.4 developing risk-mitigation tools;
 - 14.2.5 developing business-continuity plans.
- 14.3 The Board of Directors and senior management shall be involved in setting the goals of the stress tests, specifying the scenarios, discussing the outcomes, evaluating possible actions, and making decisions.
- 14.4 Senior management shall oversee the processes of developing and implementing the stress tests.
- 14.5 The stress-test results shall be disseminated to relevant lines of business and included in the considerations behind their decision-making.



15. Monitoring and reporting risks

- 15.1 The payment-system operator shall make use of methods and tools to monitor and report risks.
- 15.2 Risk monitoring and reporting shall be based on information and control systems that are able:
- 15.2.1 to provide the Board of Directors and senior management with clear, accurate, relevant, and timely information about the payment-system operator's risk profile;
 - 15.2.2 to help to detect relevant risk foci and evolving risks, including the payment system's credit and liquidity exposures and exposures to operational damage to the payment system.²
 - 15.2.3 to detect and issue an alert in cases of breach of limits;
 - 15.2.4 to facilitate the analysis of future and extreme scenarios.
- 15.3 The information and control systems shall be flexible enough:
- 15.3.1 to be easily adjusted to revisions of underlying risk assumptions;
 - 15.3.2 to reveal a risk exposure from different points of view;
 - 15.3.3 to reflect the effect of various economic and financial shocks that may affect the payment system.

16. The Risks Document

- 16.1 The Risks Document shall give a concise presentation of the risk profile such as to ascertain that the payment-system operator is compliant with the risk appetite and the risk-management framework approved by the Board of Directors.

² Said information systems shall facilitate, to the extent possible, real-time information-sharing so that participants may manage risks. If the payment system does not deliver information in real time, it shall provide participants with up-to-date, clear, and complete information during the day (as frequently as possible) and shall consider making suitable improvements in its systems.



-
- 16.2 The Risks Document shall include the following information at the very least:
- 16.2.1 description of the development of the payment-system operator's risk profile and risk determinants relative to its risk appetite, as of the reporting date and over time;
 - 16.2.2 reference, in said description, to all material risks of various kinds and shall include an analysis of external and internal determinants of material effect on the payment-system operator's current and future risk profile;
 - 16.2.3 specifics of deviations from policy and exposure limits that occurred during the reporting period and a description of management's actions to deal with them;
 - 16.2.4 results of stress tests and forward-looking scenario analyses so that it be possible to examine the payment-system operator's ability to stay within the risk appetite framework under various circumstances;
 - 16.2.5 specifics of main weaknesses and deficiencies detected in infrastructures, systems, and working processes, and their impact on the effectiveness of risk management and control, including reference to the way said weaknesses and deficiencies are treated and reportage about material mishaps that occurred.
- 16.3 The Risks Document shall underscore material risks and relate to their effect on current and potential exposures, risk appetite, and the like.

17. Incentives for risk management

- 17.1 When it constructs a comprehensive risk-management framework, the payment system shall offer participants incentives to manage and impede the risks that they pose to the payment system.³

³ Such as monetary sanctions, loss-sharing arrangements proportional to exposures posed to the payment system, and so on.



18. Recovery plan and orderly-liquidation plan

- 18.1 The payment-system operator shall identify scenarios that may deny it the ability to provide critical operations and services as a going concern and shall evaluate the effectiveness of the range of possibilities of recovery or orderly liquidation.
- 18.2 In these scenarios, the various independent and related risks to which the payment system may be exposed shall be taken into account.
- 18.3 After said review, adequate recovery and orderly-liquidation plans for periodic review and update shall be formulated; said plans shall include, *inter alia*, reference to the following:
- 18.3.1 key recovery and orderly-liquidation strategies;
 - 18.3.2 definition of the payment system's critical actions and services;
 - 18.3.3 description of the measures needed to apply said key strategies;
 - 18.3.4 ability to identify related entities in order to provide them with the information they need to apply said plans in a timely manner in the course of extreme scenarios.

19. Information reported and frequency of reportage

- 19.1 When this Directive goes into effect and no later than March 31 of each year and after the performance of any material change, the payment system shall forward the following documents to Oversight:
- 19.1.1 the risk-management framework;
 - 19.1.2 the corporate-governance structure in the context of various functions' responsibilities for risk management;
 - 19.1.3 the methods and tools used to measure and evaluate risks detected;
 - 19.1.4 the way detected risks are monitored and new risks are detected;
 - 19.1.5 recovery or orderly-liquidation plans;



-
- 19.1.6 existing incentives for participants to manage and impede risks that they pose to the payment system.
- 19.2 Periodic reporting to the Board of Directors: at least once per year, the Chief Risk Officer shall send the Risks Document to the Board of Directors risk-management committee.
- 19.3 Once per year, the payment system shall send the following to Oversight:
- 19.3.1 the Risks Document, with minutes attached of the discussion that the Board of Directors risk-management committee held in regard to it;
 - 19.3.2 a map and an evaluation of all material risks detected;
 - 19.3.3 risk appetite and risk capacity.

20. Forwarding information to the Bank of Israel

- 20.1 The payment-system operator shall forward the information under this Directive by means of secured communication (the Kasefet application). Said application shall be used after prior coordination with Oversight. Oversight may allow the information to be forwarded in other ways.
- 20.2 The information under this Directive shall be forwarded by the system operator to the contact persons whom Oversight shall appoint for this purpose.
- 20.3 A payment-system operator who forwards information under this Directive shall ascertain by telephone or by electronic mail that the contact persons referenced in Subsection 20.2 received the information.
- 20.4 A payment-system operator who sits within a Bank of Israel structure and makes use of Bank of Israel systems shall forward the information under this Directive by means of the internal electronic-mail system of the Bank of Israel.
- 20.5 Reportage to Oversight shall be carried out in digital form and not in handwriting.
- 20.6 Reportage shall be carried out in accordance with the deadlines established in this Directive. Insofar as a payment-system operator believes that a given report will not be presented by the specified deadline, he or she shall present Oversight, by electronic mail, with a written request to revise the deadline for the presentation of the report.



Said request shall include, *inter alia*, the actions taken up to said request for revision, the reasons for requesting the revision of the reporting deadline, and the requested target date for the presentation of the report in question. A reporting deadline for which revision is not approved by Oversight shall be presented by the deadline established for said report.

21. Promulgation and update of Directive

Date of promulgation	Essence of update
April 25, 2018	Promulgation of directive (Directive 6, Comprehensive Risk Management Framework)
December 24,2018	Update (Directive 6, Comprehensive Risk Management Framework)
April 3, 2024	Update (Directive 17d replaces Directive 6, Comprehensive Risk Management Framework)

The translation is intended solely for the convenience of the reader. This translation has no legal status and although every effort has been made to ensure its accuracy, the Bank of Israel does not assume any responsibility whatsoever as to its accuracy and is not bound by its contents. Only the original Hebrew text is binding and the reader is advised to consult the authoritative Hebrew text.