INFORMATION TECHNOLOGY MANAGEMENT

CONTENTS

ONLY THE HEBREW VERSION IS BINDING

CHAPTER A: GENERAL

Introduction

1. (a) The information technology system is a central component in the operation and proper management of a banking corporation, in view of the information and all its aspects and implications having a substantial impact on the banking corporation's stability and development.

(b) Due to these factors a banking corporation's management must attribute the appropriate importance, both in its managerial hierarchy and in the necessary financial resources and human resources, for the proper management of information technology system.

(c) Without prejudice to the generality of the aforegoing, this directive that includes detailed and general guidance, has been established.

(d) This directive accords with the principles for e-banking published by the International Committee on Banking Supervision (Basel Committee) in July 2003.

Application

2. This directive shall apply to banking corporations and also to corporations as provided in Sections 11(a)(3a), 11(a)(3b), and 11(b) of the Banking (Licensing) Law, 5741-1981, that were incorporated in Israel (hereinafter, a banking corporation).

CHAPTER B: SUPERVISION AND MANAGEMENT

Board of Directors

3. (a) A banking corporation's board of directors shall hold a periodic discussion and determine the banking corporation's information technology management policy pursuant to the provisions of Section 6(d) of Proper Conduct of Banking Business Directive No. 301 (Board of Directors).

(b) The information technology management policy shall *inter alia* include reference to:

(1) Information security;

(2) Backup and recovery principles in situations of malfunctions and disasters;

(3) Outsourcing;

(4) Development policy, including by end users;

(5) Cancelled;

Management

4. (a) A banking corporation's management shall appoint one manager, either a management member or a direct subordinate to the general manager, who shall bear responsibility for the entire range of information technology issues (hereinafter, the information technology manager). The said manager shall have appropriate professional training and proven experience in the information technology field and the management thereof.

(a1) Notwithstanding the stipulation in Subsection (a) above, the Supervisor of Banks may allow, in exceptional cases, the information technology manager in a banking corporation to serve as well as information technology manager in banking corporations controlled by said banking corporation, or in corporations as defined in Sections 11(a)(3a), 11(a)(3b), and 11(b) of the Banking (Licensing) Law.

(b) A banking corporation's management shall appoint an information security manager, as set forth in Section 9.

(c) A banking corporation's management shall hold an annual discussion on the implementation of the information technology management policy and the

budgeting thereof and shall make the required decisions, while distinguishing between short-term relevant subjects and long-term relevant subjects.

(d) A banking corporation's management shall devote an annual discussion to the implementation of the information security policy with all its aspects.

(e) In determining the organizational structure of the unit charged with information technology management in the banking corporation, and in the definition of the functions of the employees of this unit, the banking corporation's management shall maintain proper segregation of duties and authorities.

(f) A banking corporation's management shall define the types of activities and events in respect whereof warning must be given to management and other authorized bodies, including those that require a warning in real time.

Procedures

5. A banking corporation shall determine detailed procedures for every stage and for every process that deals with the management, operation, security, backup, continuity and control of information technology and shall carry out appropriate control of the performance thereof. These procedures shall be revised on an ongoing basis in accordance with the changes that occur in the relevant business environment and also in the technological environment.

Documentation, Record Keeping and Monitoring

6. (a) A banking corporation shall keep appropriate and current documentation for its information technology system.

(b) (1) A banking corporation shall maintain an audit trail that shall be based upon computerized recording (log) of access and transactions and queries performed in the banking corporation's information systems that shall *inter alia* include the identity of the access authorized person, the place, time and also particulars of the access subject.

(2) Notwithstanding the provisions of Paragraph (1) above, with regard to queries of the banking corporation's employees, the banking corporation shall maintain an audit trail, at its discretion, based on the risk assessment.

(3) A banking corporation shall determine the period of time for retaining the records as provided in Paragraph (1), provided that the period of time for

retaining the records shall not be less than 60 days for queries records and 6 months for transactions records.

(c) A banking corporation shall inform its customers and its employees of the existence of retention processes of their activities.

(d) Subject to the provisions of Section 4(f), the records management systems shall give warnings to the designated entities of unauthorized external activities and also of exceptional activities by the various types of users.

Internal Audit

7. (a) A banking corporation shall include within the context of its internal audit, an organizational unit for auditing its information technology. The person responsible for the internal audit in the information technology field shall have relevant professional training and experience to carry out the audit in this field.

(b) A banking corporation shall provide the internal audit with the tools required to carry out auditing and control in the information technology environment.

(c) In any event in which internal audit outsourcing is used in the information technology field, the assessment ability of the banking corporation's internal audit must be preserved.

CHAPTER C: RISKS

Risk Assessment

8. (a) A banking corporation's management shall carry out a risk assessment of the information technology system. The risk assessment must address all the potential risks connected with managing the information technology system, such as:

- The internal and external users of the banking corporation's system;;
- The system's environment;
- The system's operation and its implications on the corporation's business;
- The sensitivity of the information;
- Outsourcing.

(b) The risk assessment process shall be ongoing and the risk assessment shall be revised in accordance with changes in the various risk factors.

(c) The banking corporation shall, in accordance with the risk assessment, take the necessary measures to minimize the possibility of impairment to the information technology system and all its parts and to minimize potential damage.

CHAPTER D: INFORMATION SECURITY

Information Security Manager

9. (a) (1) The information security manager shall be subordinate to a member of the banking corporation's management.

(1a) Notwithstanding the stipulation in Subsection (1) above, the Supervisor of Banks may allow, in exceptional cases, the information security manager in a banking corporation to serve as well as information security manager in banking corporations controlled by said banking corporation, or in corporations as defined in Sections 11(a)(3a), 11(a)(3b), and 11(b) of the Banking (Licensing) Law.

(2) The information security manager shall not engage in functions that may create a conflict of interests, and in such regard he shall not be the information technology manager.

(3) A banking corporation's management shall determine the information security manager's fields of responsibility and the subjects decisions in respect whereof require his consideration. The fields of his responsibility shall *inter alia* include:

- Overall responsibility for the implementation of the information security policy in the banking corporation;
- Development and monitoring of the implementation of the information security plans in the banking corporation and examination of the effectiveness of the information security system;
- Dealing with exceptional information security events.

(4) A banking corporation's management shall provide the information security manager with the resources required for the performance of his duties.

(b) An information security manager shall have relevant professional training and experience in the field.

Information Security

ONLY THE HEBREW VERSION IS BINDING

10. (a) A banking corporation's management shall coordinate the information security principles in a document that shall be brought for the board of directors' approval. This document shall be revised periodically.

(b) A banking corporation shall implement security means - physical and logical, for the prevention, detection, rectification and documentation of exposures in the information technology system and the reporting thereof, in accordance with the risk assessment and also addressing the following aspects:

(1) Identification and authentication;

(2) Privacy;

(3) Integrity;

(4) Non-repudiation.

(c) A banking corporation shall routinely monitor the technological developments and adapt the security level and the control of access to its systems in accordance with changes in the risk level that emanates from such technological changes.

(d) A banking corporation shall act to separate the production environment from the development and test environment.

Security Survey and Controlled Penetration Tests

11. (a) (1) Periodically, in accordance with the risk assessment, the information security manager shall initiate a security survey of the banking corporation's information technology system (hereinafter, the survey). The survey that shall be carried out shall assess the effectiveness of the protection means, having regard to the risk assessment, and ways of rectifying deficiencies that will be found shall be proposed.

(2) With regard to systems that were defined by the banking corporation as being of high risk, including e-banking systems, a survey must be carried out in the format set forth in paragraph (1) above prior to implementing significant changes in such systems, when significant changes occur in the technological environment in which the systems operate, and also in anticipation of new systems as aforesaid being put into use, and at least once every 18 months.

(3) The survey's results shall include a detailed report of the findings and recommendations and a management summary that shall present the principal aspects thereof.

(b) The information security manager shall initiate controlled penetration tests into the banking corporation's information technology system to examine its resistance to internal and external risks. This operation shall be carried out at a frequency that accords with the various systems' specific risks, in accordance with the risk assessment.

(c) (1) The security survey and the controlled penetration tests as aforesaid shall be carried out by professional and independent entities, who are not part of the banking corporation, while avoiding conflicts of interests and taking the obliged cautionary measures.

(2) A banking corporation's management shall complete its discussions on the findings of the security survey and the controlled penetration tests and the implications thereof and shall make the necessary decisions, including determining a timetable for the implementation thereof, within a reasonable period of time after the time of the commencement thereof.

(d) Substantial findings that arose in the security survey and the controlled penetration tests shall be brought to the knowledge of the board of directors or an appropriate board of directors' committee.

Access Control

12. (a) (1) A banking corporation shall perform a unique personal identification of every entity with access to an information system (hereinafter, access authorized person) as a condition precedent for granting the access.

(2) Notwithstanding the provisions of paragraph (1) above, in exceptional situations of suppliers and employees in respect whereof it is not possible to effect the aforegoing, the banking corporation shall apply appropriate alternative measures.

(b) (1) A banking corporation shall determine rules and tools for the identification of and the grant of authorizations to various entities for access to components of the information technology. These rules shall

take into account the risk levels derived from the range of the user's responsibility and authority (according to a classification into groups), from the application itself, the sensitivity of the information and other information technology components.

(2) The classification into users' groups shall relate to the internal entities in the banking corporation and to the external entities (including customers, suppliers, etc.).

(3) A banking corporation shall put into operation tools for the management and control of the authorizations system.

(4) The means of access control to the information systems shall be with accepted techniques in such regard.

(c) (1) For the purposes of controlling access to information systems that were assessed as having a high risk, and in every case of remote access to the banking corporation's information technology system by employees, suppliers and service providers, the banking corporation shall use a technology that combines identification and authentication of the user, privacy and integrity of the data and non-repudiation.

(2) Notwithstanding the provisions of paragraph (1) above, a banking corporation may use alternative technology in the following events:

- In high risk systems other than via remote access, at the banking corporation's discretion, that shall be documented;
- In remote access by suppliers and service providers, where the use of technology as aforesaid is not possible for reasons that do not depend on the banking corporation.

(d) A banking corporation shall determine criteria for operating a time-out mechanism after a period of time in which there was no activity by the access authorized person. The period of time shall be determined with regard to the risk assessment.

(e) Notwithstanding the provisions of Sections (a)—(c) above, the relevant sections of Proper Conduct of Banking Business Directive no. 367 on "E-banking" shall apply to customers using e-banking services as defined in Proper Conduct of Banking Business Directive no. 367.

Encryption

13. A banking corporation shall examine the need for encrypting data, including over the communications link, and in systems that were defined in the risk assessment as being of a high risk, provided that there shall be encryption in the following cases:

(a) Cancelled.

(a1) Cancelled.

(b) Remote access to the banking corporation's computer, subject to the provisions of Section 12(c). The provisions of this section do not apply to customers using E-banking services as defined in Proper Conduct of Banking Business Directive no. 367 on the issue of "E-banking".

(c) Access authorized persons' passwords.

The Banking Corporation's Connection to the Internet

14. (a) A banking corporation shall take measures to locate imitations of its Internet website and shall provide the customer with appropriate tools to ascertain the identity of the banking corporation's website.

(b) The banking corporation's connection to the Internet shall only be effected in the following cases:

(1) Employees' connection to the Internet, as detailed in Subsections (c) and (d);

(2) Providing e-banking services, as detailed in Proper Conduct of Banking Business Directive no. 367 on the issue of "E-banking";

(3) Other use approved in advance by the Supervisor, as provided in Section 30(a).

(c) A banking corporation's management shall determine the uses permitted for the banking corporation's employees' connection to the Internet, based on the risk assessment and through taking appropriate control measures, and subject to the provisions of Subsection (d).

(d) The banking corporation's employees' connection to the Internet from work stations shall be permitted upon the fulfilment of one of the following:

(1) The work station is connected only to the Internet or to a network that is connected only to the Internet (stand alone) and there are no banking applications or sensitive information therein;

(2) The connection to the Internet shall be effected via a separate server of the banking corporation and shall be routinely controlled by the means set forth in Subsection (e). In this configuration, connection to the Internet shall be effected for purposes of surfing and electronic mail only.

(e) Pursuant to the provisions of Section 10(c), the connection of the banking corporation's network to the Internet shall be secured at least by an antivirus, content-filtering, Intrusion Detection Systems (IDS) and a firewall.

(f) The banking corporation shall, in accordance with the risk assessment, apply computerized means for application control and scanning for weaknesses of the system.

(g) The provisions of Subsections (e) and (f) shall apply on all of the banking corporation's sites, including the marketing site.

CHAPTER E: BACKUP AND RECOVERY

Discussion by Management

15. (a) From time to time a banking corporation's management shall hold a discussion on the backup and recovery principles and shall make decisions in this area, with detailed reference to the risk assessment and the following matters:

(1) Definition of malfunction situations (including at the banking corporation's suppliers) and disasters (including natural disasters, fires, war and emergency) for all the organizational units and the implications thereof on the banking corporation's continued operations;

(2) Determining the critical business processes in situations of malfunctions and disasters, the relevant information systems for the operation thereof and the mode of such system's operation in situations as aforesaid;

(3) The various software, hardware and communications components;

(4) Aspects of the backup and recovery, including reference to routine backup, backup duration, backup frequency, backup media, maximum down times and the process of returning to routine work;

(5) Reliance on external entities at the time of interruptions to the normal operation of the information systems and the recovery time required by the banking corporation to return the information systems to normal operation.

(b) Within the context of the discussion, a decision shall be made as to the routine backup arrangements (including manpower and documentation backup) and investments in backup facilities and in other backup arrangements for significant systems that were determined in accordance with the provisions of Subsection (a)(2) above.

Backup and Recovery Arrangements

16. (a) (1) A banking corporation shall maintain a detailed plan for operating its information technology system in cases of malfunctions and disasters (hereinafter, disaster recovery plan), as provided in Section 15.

(2) A banking corporation shall examine and revise the disaster recovery plan in accordance with the changes that have occurred in the period that

elapsed since the previous revision (including changes in the emergency provisions and in the risk assessment) at least once every two years and also at the time of effecting a significant change.

(b) At least once every two years and also at the time of effecting a significant change in the emergency provisions, a banking corporation shall test all its backup and recovery arrangements.

(c) The storage of backup equipment, vital software and information shall be at a location that is distant from the original storage location, so that events such as a natural disaster, war and the like shall not simultaneously damage the original and backup equipment, software and information and shall not prevent the use thereof.

(d) A banking corporation shall take measures that shall ensure the possibility of reconstructing information from backup copies, including information retained in means that are no longer being used.

CHAPTER F: OUTSOURCING

Cancelled.

CHAPTER G:

Cancelled.

CHAPTER H: MISCELLANEOUS

Foreign Bank

29. The directive shall apply *verbatim* to a foreign bank, save for the changes set forth below:

(a) Throughout the directive the expression "information technology system" shall be replaced by the expression "the local information technology system, including the interfaces of such system with the bank's system abroad".

(b) Section 3 shall apply to the management in lieu of the board of directors.

(c) The following sentence shall be added to Subsection 11(a)(3):
"A copy of the managerial summary shall be sent for the knowledge of the person responsible for the information security at the parent bank".

(d) The following section shall be added to Section 16 of the directive:
"(e) A foreign bank shall at all times retain in the local information systems at its branches in Israel full data containing all the personal and administrative particulars as to the owners of the accounts, the legal representatives and the signatory rights and also all the current balances of the accounts being conducted at its branches in Israel."

(e) The sections specified below can be effected by the parent bank and not directly by the foreign bank, provided that the foreign bank shall, if necessary, also make the necessary adaptations to comply *verbatim* with the following sections of the directive: 5, 6(a), 6(b), 7, 8(a), 10(a), 10(b), 12, 13, 14, 16(d), and to meet the provisions of Proper Conduct of Banking Business Directive no. 367.

(f) In exceptional cases, a foreign bank that believes that certain sections of this directive are not applicable to it, may apply to the Supervisor in order to adapt the applicability thereof and/or the mode of the application in respect of it, as provided in Section 30(a).

Operations Requiring Consent and Operations Requiring Reporting

30. (a) A banking corporation wishing to perform one of the following operations shall give prior notice to the Supervisor. If the Supervisor does not notify the banking corporation of non-approval of the operations within 90 days, the banking corporation can deem such to be approval:

(1) Cancelled;

(1a) Appointing an information technology manager as listed in Section 4(a1) and/or appointing an information security manager as listed in Section 9(a)(1a).

(1b) Cancelled.

(2) The banking corporation's connection to the Internet pursuant to Section 14(b)(3);

(3) Cancelled;

(4) Cancelled;

(5) Adapting the applicability of sections of the Directive for a foreign bank as provided in Section 29(f).

(b) A banking corporation shall report the following subjects and events to the Supervisor of Banks:

(1) Technological failure incidents in accordance with Proper Conduct of Banking Business Directive no. 366 on "Reporting of Technological Failures and Cyber Events";

(2) Cancelled;

(3) The establishment of an auxiliary corporation that shall engage in the information technology field;

(4) A decision as to anticipated significant changes in the information technology management policy, material conversion of the computerized systems and re-computerization of central systems and their like;

(5) Cancelled;

(6) Cancelled.

(c) Notices and reports pursuant to Sections 29 and 30 above have to be sent to the IT Regulation and Examination Unit at the Bank of Israel's Banking Supervision Department.

(d) Reports pursuant to Sections (b)(3) and (b)(4) above have to be sent 30 days in advance.

(e) Cancelled.

ONLY THE HEBREW VERSION IS BINDING

* * *

Revisions

Circular 06 number	Version	Details	Date
830		Original Circular	31/12/79
---	1	Integration into Proper Conduct of Banking Business Directive file	8/91
---	2	New version of Proper Conduct of Banking Business Directive file	12/95
1890	3	Update	27/8/97
2118	4	Switch of Directive 357 and 412	14/9/03
2292	5	Update	30/1/11
2334	6	Update	29/4/12
2507	7	Update	21/7/16
2579	8	Update	13/11/18
2643	9	Update	29/12/20

Revisions to Directive 412 (E-banking)

Circular 06 number	Version	Details	Date
103/16		Original Circular	25/9/88
---	1	Integration into Proper Conduct of Banking Business Directive file	8/91
---	2	New version of Proper Conduct of Banking Business Directive file	12/95
1814	3	Update	30/6/96
1822	4	Update	30/6/96
1889	5	Update	27/8/97
2118	6	Cancellation of Directive	14/9/03

ONLY THE HEBREW VERSION IS BINDING