The Banking Supervision Department

November 18, 2024

Circular C-06-2799

Attn: **Banking Corporations**

Re: Management of IT, Information Security, and Cyber Defense Risks

(Proper Conduct of Banking Business Directive No. 364)

General

1. The technological environment in which the banking system operates is rapidly evolving, and the reliance on the Information Technology (IT) system in the banking corporation, as well as the complexity of this system, has been increasing in recent years. Many banking corporations are undergoing digital transformation in order to enhance their efficiency and provide better and more diverse services to their customers. This process is characterized by the adoption of new technologies and the innovative use of existing technologies to offer new financial services to their customers and to further automate their operations.

2. However, while digital transformation brings many advantages to the financial ecosystem, it also exposes the banking corporation to a wide range of IT risks, which form part of the operational risks facing the banking corporation, including information security risks, the primary and most significant component is cyber risk. Accordingly, an adequate information technological risk management framework is a central pillar in the Banking Supervision Department's stability requirements.

3. To align the current regulatory framework for the management of information technological risks with the evolving technological environment, emerging threats, and internationally accepted regulatory practices, and given that information technology risks share many common characteristics, this Directive replaces the following three directives, which constitute the existing basis for the management framework of information technology risks: Proper Conduct of Banking Business Directive No. 357 on "Information Technology Management" (hereinafter:

"Directive no. 357"), Proper Conduct of Banking Business Directive No. 361 on "Cyber Defense Management" (hereinafter: "Directive 361") and Proper Conduct of Banking Business Directive No. 363 on "Cyber Risk Management in the Supply Chain" (hereinafter: "Directive 363").

4. However, in view of the increase in information security incidents in general and cyber attacks in particular, and their unique characteristics, including their increasing sophistication and impact, as well as the growing motivation of adversaries to adversely impact, inter alia, the systems, networks, and day-to-day activities of the banking corporation, the Directive includes dedicated sections addressing the management of information security risks, including cyber risk.
5. The purpose of the Directive is to adequately and effectively manage information technology while minimizing the occurrence of events in which technological risk materializes and results in a breach of the confidentiality, integrity, or availability of information assets. The directive serves as a uniform basis for managing all information technology risks in a technology-neutral manner, while providing the banking corporation with flexibility to manage risk in accordance with evolving technology, changing risks, and the specific threat profile of the banking corporation. Accordingly, this directive is primarily principles-based, but also includes specific guidelines where the Banking Supervision Department considers them necessary. A principle-based approach imposes increased responsibility on banking corporations and requires them to act with due caution, and to constantly improve the existing risk management framework and adapt it to the dynamic technological environment in which they operate, as well as to the evolving threat landscape.
6. The main building block used by the Directive is the banking corporation's information asset. The decision as to what will be considered an information asset is at the discretion of the banking corporation, and the application of the principles set out in this Directive is primarily based on the criticality and sensitivity of the information asset. Accordingly, the banking corporation is required to apply the Directive to information assets managed by a third parties, whether within the banking corporation's premises or outside them.

7. The Directive is consistent with the general risk management principles set forth in Proper Conduct of Banking Business Directive no. 310 on "Risk Management" (hereinafter: "Directive 310"), and the principles for managing operational risks set forth in Proper Conduct of Banking Business Directive no. 350 on "Operational Risk Management" (hereinafter: "Directive no. 350"), and is written in accordance with other Proper Conduct of Banking Business Directives that deal directly with the technological field, such as Proper Conduct of Banking Business Directive no. 362 on "Cloud Computing" (hereinafter: "Directive 362"), and Proper Conduct of Banking Business Directive No. 355 on "Business Continuity" (hereinafter: "Directive 355") or relating thereto, such as Proper Conduct of Banking Business Directive no. 359A on the subject: "Outsourcing" (hereinafter: "Directive no. 359A").

8. In the future, the Directive will serve as the basis for the Banking Supervision Department's directives on designated issues in the field of information technology, should they be published. In addition, to ensure uniformity in the use of the terms set forth in this Directive within the current regulatory framework in the field of information technology, the Banking Supervision Department intends to publish adjustments to the relevant Directives, such as Proper Conduct of Banking Business Directive no. 366 on the subject: "Reporting of Technological and Cyber Failure Events" (hereinafter: "Directive no. 366").

9. The regulation was not accompanied by the publication of a report under the Principles of Regulation Law, 5781-2021—hereinafter in this section, the "Law", in view of the exemption set forth in Section 34(c)(4) of the Law, as it is based in large part on accepted rules in countries with significant markets, and in light of the prescribed in Section 34(c)(2) of the Law, as the remaining part replaces other Proper Conduct of Banking Business Directives without material changes.

   The regulation will be subject to retroactive examination in accordance with Section 36 of the Law, at the end of 10 years from the date of its entry into force.

10. After consulting with the Advisory Committee on matters relating to banking business and with the approval of the Governor, I have established the following Proper Conduct of Banking Business Directive, as detailed below.

Structure of the Directive

11. The directive consists of sixteen chapters grouped under six sections:

11.1. **Part A: Introduction** – including **Chapter A: General** – Introduction to the directive, Application, and Definitions.

11.2. **Part B: Corporate Governance and Risk Management Framework** – Consists of three chapters:

11.2.1. **Chapter B: Corporate Governance** – Details the roles of the Board of Directors, Senior Management, Information Technology Manager, Chief Cyber Defense and Information Security Officer, Risk Management Function, and Internal Audit.

11.2.2. **Chapter C: The Information Technology Risk Management Framework (General)** – deals with the organization and objectives of the framework for managing all information technology risks, including information and cyber security risks, the processes for identifying and classifying the main building blocks required for the management of this framework, and the assessment and mitigation of risks. The identification and classification of these building blocks is a basic condition for the banking corporation's ability to meet the requirements of the Directive.

11.2.3. **Chapter D: The Human Factor – User Training and Awareness** – deals with training programs for new technologies and products, training for new employees, periodic training to refresh the knowledge of existing employees, and training and awareness programs on information security issues.

11.3. **Part C: Information Technology Risk Management** - consists of two chapters:

11.3.1. **Chapter E: Information Technology Management** – deals with the proper management of information technology, including principles for the planning, implementation, operation and control of the information technology system, the proper implementation of which will reduce information technology risks.

11.3.2. **Chapter F: Project Management and Change Management** – deals with the framework of the work for managing information technology projects, principles for acquisition management and management of system development, including the implementation of a purchased system, principles for managing the development and service of APIs, and principles for change management.

11.4. **Part D: Information Security and Cyber Defense Risk Management** - Consists of three chapters:

11.4.1. **Chapter G: Information Security** – deals with assessing the information security capability of the banking corporation and its adaptation to the scope of the banking corporation's information assets and the scope of the risks to these assets, the overarching principles on which the framework for information security management and cyber defense should be based, as well as the issues that should be addressed in the information security and cyber defense policy.

11.4.2. **Chapter H: Implementation of Information Security Controls** - Details the information security controls, including the cyber defense controls that the banking corporation must implement, while addressing the following aspects: the criticality and sensitivity of the information asset, vulnerabilities and threats to the information asset, the stage in the life cycle in which the information asset is located, minimizing exposure to severe but reasonable scenarios of information security incidents.

11.4.3. **Chapter I: Assessing the Effectiveness of Information Security Controls** – deals with the requirement to evaluate on an ongoing basis the maturity, effectiveness of the planning, implementation and operation of those information security controls implemented by the banking corporation.

11.5. **Part E: Incident Management** - consists of two chapters:

11.5.1. **Chapter J: Monitoring Information Technology**– deals with the policies, procedures, and means that the banking corporation must determine in order to identify emerging and anomalous problems, in order to prevent them from developing into technological failure events or information security incidents.

11.5.2. **Chapter K: Incident and Problem Management** – deals with processes for managing technological failure events and information security incidents.

11.6. **Part F: Miscellaneous** - It has five chapters:

11.6.1. **Chapter L: Reporting Information Technology Risks and Information Security Risks** – deals with the regular reports submitted to senior management and the Board of Directors on information technology risks and information security risks in accordance with the requirements of Directive no. 350.

11.6.2. **Chapter M: Third Party Risk Management (TPRM)** – Coordinates the specific guidelines given in the Directive regarding risk management vis-à-vis third parties (service providers to the banking corporation and suppliers, as well as other parties (other than customers) to whom the banking corporation provides service or with whom the banking corporation shares its information assets).

11.6.3. **Chapter N: Business Continuity Management (BCM)** – deals with the principles for building a disaster recovery plan (DRP) in accordance with the banking corporation's Business Continuity Plan (BCP), examining and practicing it.

11.6.4. **Chapter O: Foreign Bank –** specifies specific guidelines for a corporation that has been granted a foreign bank license in accordance with the Banking (Licensing) Law, 5741-1981.

11.6.5. **Chapter P: Reporting to the Banking Supervision Department** – specifies the required reports on information technology management to the Banking Supervision Department.

Part A – Introduction

Chapter A – General

Management of Information Assets by a Third Party (Section 5 of the Directive)

12. The definition of "third party" in this directive is broader than the definition of "service provider" in Directive 359A. Accordingly, a third party also defined as a "Service Provider" in Directive 359A is required to comply with the requirements of this directive and the requirements of Directive 359A.

Application (Section 10 of the directive)

13. The applicability of the directive corresponds to the applicability of the Proper Conduct of Banking Business Directive no. 367 on the subject: "E-Banking" (hereinafter: "Directive 367") and Directive no. 366 (changed from "Acquirer" to "Payment Service Provider with Prudential Importance".

Definitions of Terms (Section 11 of the Directive)

14. The definitions are intended to clarify the framework for the implementation of the directive and to allow for uniform language and the definition of expectations. Thus, definitions of "information technology risk", "information security risk", and "information assets" were determined, which were used throughout the directive as a central component of the control framework.
15. **"Information Security" –** the preservation of an information asset from unauthorized actions, whether carried out intentionally or inadvertently, in order to provide confidentiality, integrity, and availability.
16. **"Technological failure incident" –** the definition of this term has been moved from Directive no. 366. It should be noted that even a breach of confidentiality or failure of completeness or incompatibility or unavailability of an information asset (except for a breach of confidentiality, failure of integrity or unavailability of an information asset that has been classified as an information security incident) without the ongoing operation of the information technology system or of the

services provided by it being impaired, will be considered as a "disruptive effect on the proper operation of the information technology system".

17. **"Authorization" –** providing access to information assets for the applicant based on the needs of the banking corporation, including its business needs, compliance with the provisions of the law and the customer's requirements, as well as based on the required level of information security.

18. **"Identification (in the context of identification and authentication of a party requesting access)" –** the definition of the term is in the context of identifying and authenticating a party requesting access, and for the avoidance of doubt it does not define identification in other contexts such as the requirement in section 43.2 of the Directive regarding the identification of information assets.

19. **"Information technology, information technology system" –** In this directive, the terms "information technology" and the term "information technology system" are used as synonyms.

    It should be noted that the information technology system does not include the department's employees.

20. **"Sensitive Information" –** any information that has been classified as sensitive in accordance with the banking corporation's sensitivity classification, which is required by Chapter C of the Directive, whether this information belongs to an individual, a corporation or to the banking corporation itself (for example: information about the banking corporation's business activity), including any "information of special sensitivity" as defined in Amendment No. 13 to the Protection of Privacy Law, 5741 – 1981 (hereinafter: the "Protection of Privacy Law").

21. **"System" –** a banking corporation shall determine what it considers to be a system in accordance with this definition, for the purpose of fulfilling the requirements of the relevant sections.

22. **"Information Assets" –** Information assets are the basic building blocks in the management of the information technology system of the banking corporation, including the management of information technology risks.

The definition of information assets also includes data on printouts, and the provisions of the Directive will also apply to printouts as applicable.

23. **"Confidentiality" –** both in terms of information security and in terms of privacy protection.

24. **"Information Security Risk" –** The risk consists of the term "information security threat" and the term "information security vulnerability". Information security risk is part of information technology risk and is characterized by being created as a result of unauthorized acts of access, use, disclosure, disruption, alteration or deletion that may compromise the confidentiality, integrity or availability of an information asset.

25. **"Information Technology Risk" –** according to the definition, this risk includes information security risk, as well as risks of damage to the confidentiality, integrity and availability of an information asset as a result of natural disasters and authorized actions.

26. "**Vulnerability**" – a technological, process, or human weakness in an information asset or information security control that can be exploited for the purpose of compromising information security.

27. **"Information Technology Project" –** The use of the term "Information Technology Project" in the Directive is generic for the tasks of modification, replacement, decommissioning, etc. of Information Technology. Each banking corporation will fulfill the requirements of the Directive for the "Information Technology Project" in accordance with its terminology for performing the aforementioned tasks.

Part B – Corporate Governance and a Risk Management Framework

Chapter B – Corporate Governance

General (Section 12 of the Directive)

28. Corporate governance in the field of information technology is an integral part of the overall corporate governance of the banking corporation and consists of organizational culture, organizational structure, and processes designed to ensure

that the information technology system meets its organizational strategy and goals. The goals of corporate governance in the field of information technology are to ensure that the information technology system creates business value for the banking corporation and minimizes the risks involved in the use of technology.

29. This section is intended to ensure that all activities necessary for IT management and IT risk management (including decision-making, approvals, supervision and operation of information security and cyber defense) have been defined and assigned to the relevant individuals, including the Board of Directors and its committees.

The Responsibility of the Board of Directors for Information Technology Risk Management (Section 13 of the Directive)

30. This section is intended to emphasize the responsibility of the Board of Directors to ensure that the level of information technology, the information security of the banking corporation, and the controls implemented against other information technology risks, are not only compatible with the rapid changes in the field of technology, but also relate to the broader strategic goal, which is the continuation of the proper operation of the banking corporation. In addition, through this requirement, the Banking Supervision Department seeks to increase the involvement of the Board of Directors in the field of information technology and in information security and cyber defense of the banking corporation, and to encourage it to use, if necessary, appropriate experts in these fields.

Outlining the Information Technology Strategy (Section 14 of the Directive)

31. The information technology strategy will define a comprehensive outline that guides the management of technology in the banking corporation and contains goals and plans at a macro level for all areas of information technology that affect the banking corporation, and not only for the infrastructure. The strategy focuses on a 3 to 5 year horizon and will help ensure that the technology planning is consistent and coordinated with the business planning of the banking corporation.

32. The strategy is also required to reflect the need for dynamic management of the information technology field in the banking corporation, and its continual adaptation to the evolving situation. The rapidly changing technologies may affect

the banking corporation's activity, and what was sufficient and appropriate in the past is no longer necessarily sufficient and relevant today.

33. An effective IT strategy will ensure the provision of technological services that balance costs with efficiency, while at the same time enabling business lines to meet the competitive demands of the market.

34. In accordance with Section 14(e) of Directive 310, the risk appetite shall be formulated in clear and understandable language and shall serve as a basis for determining the policy and limits of risk.

The Board of Directors' understanding of information technology operations and risks, and its monitoring of the implementation of the information technology strategy (Section 17 of the Directive)

35. The Board of Directors is required to understand the operations of information technology at a sufficient level that will enable it to fulfill its duties, including supervising the manner in which risks are managed.

36. In light of its responsibility in accordance with Section 13 of the Directive, the Board of Directors is required to decide, for example, for which key information technology projects it wishes to receive a report, which performance indicators it wishes to receive, and which priorities are required to be submitted for its approval.

37. The banking corporation is required to link the information security capability (sections 100-102 of the Directive) to the role of the Board of Directors to ensure that information security and cyber defense correspond to the scope of threats, and that the information security capability enables the banking corporation's proper operation to continue. In this way, the Banking Supervision Department seeks to strengthen the importance of information security and cyber defense in the banking corporation and the need to address its impact on the banking corporation in a broader manner.

The Chief Technology Officer (CTO) (Sections 23-26 of the Directive)

38. The Chief Technology Officer is responsible for the information technology system, including the day-to-day operation and management of all technological activities, the information security of the information technology environment, and

its operational resilience. The Chief Technology Officer is responsible, among other things, for the availability of the components that make up the banking corporation's infrastructure, including hardware, networks, communications, software, and storage.

39. The Chief Technology Officer in the banking corporation will not be able to bear additional responsibilities, neither within the banking corporation nor outside it, that may interfere with functioning for various reasons, for example: in the event of conflicts of interest or limited resources.

40. This Directive does not require notification of the appointment of the Chief Information Technology officer (CTO), since the CTO is already included in the list of the seven additional officers of the banking corporation whose appointment is subject to the approval of the Supervisor of Banks, in accordance with Sections 11A and 15C of the Banking Ordinance. In accordance with these sections, a person shall not serve as an officer of a banking corporation or as an acquirer, unless the Supervisor has been notified at least sixty days prior to the commencement of the appointment.

Lines of business managers (Section 27 of the Directive)

41. Lines of business managers, in addition to the Chief Technology Officer (CTO) and the Chief Cyber Defense and Information Security Officer (CISO), also have responsibilities in the field of information technology. Each position holder is responsible within their respective area. For example, in the due diligence process relating to a third party, the Lines of business managers—who, among other things, is involved in defining system requirements, prioritizing development activities, ensuring the availability of backups, and documenting processes - will perform checks to ensure that the system meets business requirements, while CISO will perform checks to ensure that the system complies with the banking corporation's information security policy.

The section provides examples of responsibilities in the field of information technology that require a clear division of responsibilities among these roles. Since each banking corporation has a unique organizational structure and culture, this

division will be carried out in accordance with the banking corporation's policy and the processes established based on it.

42. The section does not relate to the manner and degree of depth in which the duties of the Lines of business managers are performed. For example, in conducting due diligence on a third party, the Banking Supervision Department has not specified the level of examination that is to be performed, and it may be determined, inter alia, in accordance with the criticality and sensitivity of the information asset.

    Insofar as a third party is also a "service provider" as defined in Directive 359A, the banking corporation must also preform the due diligence in accordance with the requirements of Sections 18-21 of Directive 359A.

43. Monitoring third-party activity by lines of business managers can take place, for example, in the form of receiving a periodic activity status report while comparing it with the third-party's obligations under the contract.

Roles of the Chief Cyber Defense and Information Security Officer (CISO) (Sections 28-34 of the Directive)

44. The section specifies the roles of the Chief Cyber Defense and Information Security Officer (CISO) and does not provide guidance as to the manner and scope of performing these roles. For example, the section states that the CISO is responsible, inter alia, for conducting due diligence in aspects of information security and cyber defense on third parties. However, the section does not relate to the level at which due diligence will be carried out and this may be determined in accordance with the possible effects of an information security incident on the information assets to which the third party has access (see Section 102.1 of the Directive).

    Insofar as a third party is also a "service provider" as defined in Directive 359A, the banking corporation must also perform the due diligence in accordance with the requirements of Sections 18-21 of Directive 359A.

45. The Chief Cyber Defense and Information Security Officer (CISO) is required to keep abreast of new business initiatives in order to identify information security risks in these initiatives, as well as to determine ways to reduce them. For this purpose, the CISO can hold a dialogue with the managers of the lines of business, as well as

learn about these risks from other sources, for example, other entities that have implemented these initiatives and other parties in the industry.

Similarly, the CISO must also keep abreast of information flow processes, the risks to information in these processes, and the necessary information security and cyber defense measures, through dialogue with line of business managers, other entities in the organization, and sources outside the organization.

46. An example of coordination and liaison with external parties on cyber defense issues is participation in the national CERT's forums and knowledge-sharing groups and other cooperation programs in which information security and cyber threats are monitored, shared, and discussed.

    The sharing of information and intelligence for defensive purposes with external parties will be carried out in accordance with the law, including the instructions of the Supervisor of Banks (see section 111.4 of the Directive).

47. There's a difference between "integration of incident management"" and "incident management". Under the requirement to "integrate the management of the incident", the Chief Cyber Defense and Information Security Officer (CISO) is required to ensure that all the relevant parties are "around the table" and that the banking corporation is acting according to the existing contingency plans. In addition, the CISO is required to fulfill its role as an advisory function to senior management and the Board of Directors on various issues that may arise, etc. A banking corporation may determine, depending on the characteristics of the incident, the identity of the party responsible for managing the incident. However, the integration of incident management must be carried out by the CISO.

The work plan of the internal audit (Section 37 of the Directive)

48. The internal audit is an important tool through which the board of directors can ensure that the technological controls are implemented in such a way that they reduce the risk and operate in the way that the management of the banking corporation has planned. For example, the Board of Directors can use this tool to ensure that the information security is maintained in the banking corporation. To this end, the internal audit must address the various aspects of information technology, including the information security aspects, as part of its work plan. Of

course in some cases, for example, when the internal audit does not have the appropriate knowledge and expertise, or when the subject under review is managed by a third party, in order to complete the picture provided by the internal audit, the Board of Directors may also choose to rely on expert opinions or other means of its choice.

The internal audit will map out all the activities of the information technology (IT) system, corporate governance, functions and processes in the field of information technology, including those in the field of information security. This mapping will serve as the basis from which the internal audit work plan is derived.

Reliance of the internal audit on work performed by another party (Section 38 of the Directive)

49. The section refers to cases in which the internal audit relies on work performed by parties outside the internal audit function in order to carry out its responsibilities. In such cases, the internal audit must evaluate the scope and quality of the examination performed, in order to determine whether and to what extent it can be relied upon. Following are the cases:

    49.1. Reliance of the internal audit on work performed by other parties within the banking corporation. For example: a review of the planning and effectiveness of information security controls conducted by the Chief Cyber Defense and Information Security Officer (CISO).

    49.2. The use of the internal audit to be outsourced for the purpose of carrying out the activities assigned to it.

    49.3. Reliance of the internal audit on examinations provided to it by a third party that performs activities on behalf the banking corporation.

Chapter C - IT Risk Management Framework (General)

General

50. Further to Section 9 of the Directive, the Information Technology Risk Management Framework will be aligned with the risk management framework required by Directive 310.

This chapter serves as an overall framework for managing all information technology risks including information security risks facing the banking corporation. The main focus of this chapter is the obligation of the banking corporation to establish a methodology for identifying information assets, business activities and supporting processes, as well as for measuring and mitigating risk. The chapter also addresses the requirement for the allocation of responsibilities for risk management, including the allocation between the three lines of defense, key roles, and reporting lines.

Information Technology Risk Management (Section 41 of the Directive)

51. The section corresponds to the order of actions in risk management: identification, evaluation, control, monitoring, and reporting, with Section 41.7 of the Directive specifying the reasons for the start of a new cycle of updating risk management.

52. There may be technological failure incidents or information security incidents that will be defined by the banking corporation as significant for the purposes of identifying and assessing new information technology risks, but they will not be obligated to report to the Banking Supervision Department according to the reporting criteria specified in Directive 366. In addition, a significant technological failure incident and a significant information security incident in this section are not necessarily the incidents that are the subject of section 146.6 of this directive.

Identification and classification of activities, processes, and information assets (Section 43 of the Directive)

53. Regarding the level of detail of the mapping required—see Section 44 of the directive.

54. For the avoidance of doubt, the identification of all business activities in accordance with this section can also be used for the purpose of mapping the critical processes and services under Directive 355.

55. A banking corporation can derive added value from understanding the relationships between information assets, including identifying assets that are not classified as highly critical or sensitive but could be used to compromise the information security of highly critical or sensitive assets, or whose technological failure could impact such assets

56. Needless to say that, as a precondition for mapping all information assets managed by a third party as required by the Directive, the banking corporation must map all "third parties" as defined in this Directive.

57. In order to effectively manage the information technology risk, the banking corporation must fully identify and understand its information assets, and the impact of a potential adverse effect on their information security or a technological failure affecting them. Accordingly, all information assets of the banking corporation, including infrastructure, secondary systems such as physical access control systems, as well as information assets managed through a third party, must be identified and classified according to their level of criticality and sensitivity.

58. To simplify the process of identifying information assets and mapping the relationships between them, the banking corporation can make use of appropriate database management systems such as Configuration Management DataBase (CMDB), which are systems that manage information about the organization's information assets, including the relationships between them.

59. It is very essential to keep the mapping and classification of business activities, supporting processes, and information assets up to date in terms of criticality and sensitivity. An out-of-date product may impair the information technology risk management processes, including the information security risk management processes of the banking corporation. Accordingly, the banking corporation is required to carry out a process:

    - To identify cases where a change in the classification of information assets, business activities, or supporting processes is required.
    - To classify new information assets, business activities, or supporting processes.

    This process must be carried out in each of the following cases:

    - At least once a year—the annual process will serve as a control for the ongoing accuracy and completeness of the mapping and classification products' as stated above, and for the identification of other errors and failures in the products, if any.

- When material changes are made to information assets, business activities, and supporting processes—such changes may affect the classification of information assets, business activities, and supporting processes that are not necessarily those in which the changes were made. Such a process may identify these effects.
- When changes are made in the business environment in which the banking corporation operates.

Methodology for identifying and classifying business activities, supporting processes and information assets (Section 44 of the Directive)

60. The level of detail of the mapping of the information assets will be determined by the banking corporation in such a way that the mapping will enable the determination of the nature and strength of the controls required to protect these assets. For example, a system can be viewed as a collection of its components (applications, databases, operating system, middleware, data), and can be treated as a single information asset for mapping purposes, or alternatively, each of its components can be treated as an information asset in itself.

61. Classification in terms of criticality and sensitivity shall take into account, inter alia, the impact of a possible breach of information security on the information asset or the impact of a technological failure on the information asset. As the term "criticality" is defined in the directive as "the potential impact of the lack of availability", the classification of the information asset is also affected by the degree of its importance to the maintenance of the critical processes and services defined in the banking corporation's business continuity plan.

    The level of criticality and the level of sensitivity with which each information asset is classified do not have to be the same.

Information Asset Owner (Section 45 of the Directive)

62. The owner of the information asset will usually be an employee in the business function that requires the information asset more than the other entities that use it. The responsibilities of the owner of the information asset shall be defined, and the owner will be required to report, inter alia, regarding the information security of the asset.

It should be clarified that even if a database as defined in the Privacy Protection Law is defined by the banking corporation as an information asset, the banking corporation is not obligated to determine that the owner of the information asset will also serve as the manager of the database as defined in the Privacy Protection Law, and vice versa.

Conducting a risk assessment on an ongoing basis (Section 46 of the Directive)

63. As stated in Section 9 of the Directive, the information technology risk management process, including the risk identification and assessment stage, is required to comply with the operational risk management principles detailed in Directive 350 and the general risk management principles set forth in Directive 310. In addition, in the process of identifying and assessing information technology risks, additional emphases shall be applied as detailed in this section**.**

Chapter D - The Human Factor

Definition of "employees" (Section 50 of the Directive)

64. For the avoidance of doubt, the term "employees" in this chapter includes external employees managed by the banking corporation.

Continuity in key positions in the information technology system (Section 52 of the Directive)

65. The goal of maintaining continuity in key roles is to provide a smooth transition in the event of turnover in essential management or operations roles.

A program for training and raising awareness on information security issues (Section 53 of the Directive)

66. To reduce human error, theft, fraud, improper use of an information asset, or losses, the banking corporation shall develop a program for training and raising awareness on information security and privacy protection, which will be passed periodically and at least once a year, for all employees, including external and temporary employees.

    The training and awareness program on information security and privacy protection may include, among other things, addressing the following topics: the use of information assets for personal vs. work purposes; the use of email and the

Internet (including social networks) and malware protection; physical security, including on printouts at the employee's home; remote access (especially from unprotected environments) and the use of mobile devices; awareness of common attacks directed at the employees and facilities of the banking corporation (for example: Social engineering; tailgating; access controls including password rules and other authentication requirements; development by end users; expectations from employees when it is possible to use the employee's device (Bring Your Own Device); handling of sensitive information and data; reporting information security incidents and suspected information security incidents.

Part C - IT Risk Management

General

67. This part of the Directive deals with information technology management and the risks associated with it (see the definition of "Information Technology Risk" in Section 11 of the Directive). Part D of the Directive deals with the unique aspects of information security risks, including cyber risks.

Chapter E - Information Technology Management

Information Technology Management Policy (Section 54 of the Directive)

68. Effective IT management is an essential part of IT risk management. The principles and practices that make up the planning, implementation, and operation processes detailed in this chapter below, and which will be reflected in the information technology policy, are important for creating an effective technological environment. They support the banking corporation's lines of business and the providing of products and services in order to meet the objectives of the business strategy. Insufficient coordination and supervision of the planning, implementation, and operation processes may lead to the realization of a variety of risks such as: credit risk, liquidity risk, operational risk, and compliance risk.

Features of Information Systems (Section 55 of the Directive)

69. Various information systems provide management and the Board of Directors with the information necessary for the effective management of the banking corporation. The banking corporation's management and the Board of Directors use information systems for the purposes of evaluating the business performance of the banking corporation, reporting on the risks and challenges it faces, and mainly for the purpose of assisting in its business management.

70. Information systems provide data to decision makers while enabling them to carry out their duties, support and improve decision-making processes, and improve work performance in the banking corporation.

71. At the Board of Directors and senior management levels, IT reporting provide data and information that helps make strategic decisions. At the other levels, the information system reports enable management to monitor the activities of the banking corporation and disseminate information to employees, customers, and management members.

72. The improvement in technology has brought with it an increase in the volume of data and information available to management and the Board of Directors for planning and decision-making. Since the input of the information systems can be entered manually or from information produced from a large number of financial systems, the banking corporation is required to implement appropriate control procedures in order to ensure that the data and information produced from the information systems are correct and relevant.

73. Since information system reports can come from multiple technology platforms, controls should be designed to maintain the integrity of the information and processing environment.

    Accordingly, for IT reports to serve as an effective tool for the Board of Directors, management, and employees, they must meet five essential elements:

    - Punctuality —In order to carry out a quick decision-making process, the information systems of the banking corporation must be able to provide and disseminate up-to-date information to the relevant parties.

- Accuracy – Information systems need to provide accurate data, and for this purpose the banking corporation can use internal automated and manual controls in the information systems in order to verify the validity of the data.
- Consistency – In order for the information to be reliable, the data needs to be processed in a uniform manner. Using a variety of information collection methods and a variety of reporting methods in an inconsistent manner may adversely impact information and trend analysis.
- Completeness – Reports should include the information necessary for decision makers without excessive detail.
- Relevance – Information systems must provide up-to-date, applicable, and actionable information.

Operational Resilience (Section 56 of the Directive)

74. A secure and resilient information technology system, which includes architecture processes, building a technological infrastructure, and appropriate operations, is essential for the delivery of the essential activities by the banking corporation. To strengthen the operational resilience of the banking corporation, the banking corporation is required to integrate these processes into its business continuity plan, so that they will help reduce threats, respond to and recover from disruptions, and learn lessons.

75. The operational resilience of such processes (architectural planning, building technological infrastructure, and operations) goes far beyond mere recovery capabilities. Operational resilience is achieved by taking proactive steps to maintain confidentiality, integrity and availability and reduce the risk of disruption, when planning an appropriate information technology (including backup and recovery systems), appropriate selection of technological infrastructure, and actual deployment of the system. A banking corporation is required to plan, implement, and operate the IT and the processes it operates, so that they provide operational resilience for essential business activities.

76. To properly integrate aspects of operational resilience, in the processes of planning and updating the architecture, and in the implementation of the technological infrastructure, the banking corporation will ensure that these aspects

are integrated into the project management process that it has set for itself. Integrating these aspects into the formal processes practiced by the banking corporation can assist in strategic decision-making processes and in allocating resources to strengthen the operational resilience of the core business lines (the banking corporation's lines of business, including related activities, services and functions, which, according to the banking corporation's assessment, failure occurring with them would result in a significant loss of income or profit).

Architecture (Section 57 of the Instruction)

77. Planning and designing an effective information technology architecture will assist management in building a technological infrastructure that is in line with the banking corporation's business goals, strategies, and objectives.

78. As stated in Section 56 of the Directive, a banking corporation is required to address aspects of operational resilience (e.g., redundancy, multi-layering, and robust backup systems), including aspects of information security and cyber defense, at the very beginning of the architecture design process.

79. There are a variety of methodologies for developing an information technology architecture program. The guiding principle in all of them is that large parts of the technology requirements are the result of a pre-planned process that begins with the business requirements and ends with technological solutions that are in line with the policies and procedures approved by senior management and the Board of Directors. An effective information technology architecture program may help, among other things, in the following areas:

    - Improving the use of information technology for the purpose of creating business adaptability for the banking corporation.
    - Creating a close partnership between the lines of business and the organizational units responsible for information technology.
    - Improved focus on the goals of the banking corporation.
    - Reduction in the number of system downtime incidents.
    - Reduce the complexity of systems.
    - Improving the agility of information technology.
    - Better match between what the IT array provides and business requirements.

- Ensuring that all software, including operating systems, are up to date and that support services are not about to expire.

80. Key points to consider when developing an IT architecture plan include, but are not limited to, information security and cyber defense, business resilience, data management, connectivity to entities outside the banking corporation, and alignment with the banking corporation's goals and objectives. In order to effectively implement the plan, the banking corporation needs to analyze the risks and potential impact of threats on all banking corporation activities. A comprehensive plan based on good practices can help the banking corporation develop processes for managing miscellaneous information technology-related issues, and to identify, measure, and implement controls against the various information technology risks.

Technological Infrastructure (Section 58 of the Directive)

81. The following are examples of implementing technology infrastructure controls:

81.1. Hardware –

81.1.1. Managing an up-to-date inventory of all hardware components in the banking corporation that will help the banking corporation protect them, manage information security risks, respond to incidents and recover from them. For this purpose, a banking corporation can use appropriate automated tools.

81.1.2. A process for identifying unauthorized information assets connecting to the network, and for formalizing their handling (removal, isolation, or inclusion in the updated asset inventory).

81.2. Networks and Communications –

81.2.1. A process that documents and maintains an up-to-date inventory of hardware and software that make up the banking corporation's networks and communications, as well as the configuration of the network, including a process for reviewing and managing changes in networks and communications.

81.2.2. A process that verifies the existence of redundancy for the communication infrastructure.

81.2.3. A process that verifies the compliance of the banking corporation's communication infrastructure with current and expected network traffic data.

81.2.4. Physical security of communication equipment and restricting and monitoring access to it by establishing appropriate policies and procedures.

81.3. Software –

81.3.1. A process for locating and monitoring the software in the banking corporation, whether it is network-based or located in the employee's workstation.

81.3.2. Use of tools to manage the software portfolio in the banking corporation.

81.3.3. Portability – a feature attributed to software that can operate with minimal modifications, on operating systems different from the operating system for which it was created.

82. The technological infrastructure will support operational resilience in accordance with the criticality of the information asset for the essential activities of the banking corporation. For example, a banking corporation will choose between server redundancy, an alternative website, or an alternative service, to provide an appropriate level of operational resilience in accordance with the criticality of the information asset.

Principles for Managing Operations (Section 59 of the Directive)

83. The operational process is the execution of activities consisting of methods, principles, processes, procedures, and services that support the business activity

of the banking corporation. The operational environment includes the systems and facilities that the banking corporation uses to carry out its business and operational processes. The operational environment executes routine and supporting processing activities across various functions within the banking corporation, including the provision and management of services, as well as control processes, in order to achieve the corporation's objectives. As part of the framework for managing the operations of the information technology system, and because of the need to embed operational resilience aspects within it, a banking corporation shall implement within the operational environment processes and controls across four key domains: operational controls, operational technological processes, service and support processes, and monitoring and evaluation processes.

Operational Controls (Section 60 of the Directive)

84. Operational controls are all the day-to-day procedures and mechanisms that are designed to protect the operating systems and software of a banking corporation. Operational controls affect the systems and software environment. As the systems and software environments are the foundations on which the banking corporation's business processes are based, the management of the banking corporation should define processes and implement controls to protect these environments. These controls include, but are not limited to, physical and logical controls on the use of banking corporation facilities, controls for identity management and access to information assets, controls on the human factor such as: strict screening processes to ensure the employee's suitability for the job, orderly definition of roles and areas of responsibility, implementation of rotation in various roles, proper separation of roles, implementation of the four-eye principle, and controls for the use of the employee's private equipment. A breakdown of some of the controls included under this group appears in Chapter H of the Directive "Implementation of Information Security Controls".

Maintenance Processes (Section 61.1 of the Directive)

85. Preventive maintenance reduces the failure incidents of equipment and can diagnose problems before they occur. A banking corporation is required to implement various maintenance processes to prevent such failures, for example: a review of a periodic report that includes data such as the frequency and type of problems discovered from the activity log of the information asset, can help identify potential problems that require a system replacement, or a vendor replacement, or an increase in the capacity of the information asset, etc.

End of Life/End of support (Section 61.3 of the Directive)

86. Proper management of the information asset life cycle includes, among other things, maintaining support for it and minimizing its vulnerabilities. Various technological risks, including information security exposures, can result from outdated hardware or software, or from limited support or lack of support at all, whether it is supported by a third party or in-house. A technology that is approaching the end of its lifecycle (i.e., no new investments are being made in it), for which support has been discontinued or is nearing its end-of-support period, is generally less secure by design, and cannot be updated against emerging threats within a reasonable timeframe, if at all.

    When support arrangements exist for a period beyond the date of the end of the official support for the information asset (hereinafter "Extended Support Arrangements"), it is important for the banking corporation to have a clear understanding of the nature of those arrangements and their effectiveness. In addition, while extended support arrangements or those that are specific to the banking corporation itself can partially minimize risks, they are usually expensive, and can give a false sense of a solution, including a false sense of information security or worse, postponing the treatment of obsolete technology. Furthermore, these types of support arrangements typically provide patchwork for only critical vulnerabilities, remaining constrained by the limitations of the aging technology.

Patch Management (Section 61.4 of the Directive)

87. Patch management is a process in which required repairs in operating systems and system code are identified, the repairs are validated, and finally implemented.

These processes are the joint responsibility of the operational bodies and the information security and cyber defense function. In accordance with the general requirement in Section 15(c) of Directive no. 310, according to which an appropriate internal control environment on which the framework for risk management in the banking corporation will be based must be anchored in clear procedures, the banking corporation is required, inter alia, to establish procedures for the purpose of constantly updating patches against the various vulnerabilities, procedures for examining patches in a separate environment, and procedures for installing them.

In a case where a change is required as an emergency response for which the normal patchwork management process cannot be implemented—see Section 97 of the Directive.

Backup Management (Section 61.5 of the Directive)

88. Backups allow the banking corporation to resume operations within a predefined period of time, while allowing business continuity with limited disruption. The decision to implement a specific method of backups will be based, among other things, on the criticality and sensitivity of the data and systems that constitute the information asset.

89. Regarding backups – see also reference in Directive 355.

Capacity and Performance Management (Section 61.6 of the Directive)

90. The process of capacity management is the process of planning and monitoring the technological resources of the banking corporation required to support its current and expected strategic objectives. The process uses the current capacity data of the information technology system for the purpose of modeling and forecasting the future needs of the banking corporation. Capacity management should be closely integrated with the budgeting and planning processes of the information technology system—see Section 64 of the Directive on the subject of "IT planning and investment process".

The manner in which the capacity management process will be carried out is at the discretion of the banking corporation, but it is recommended that the process

be carried out using automated tools in order to make it easier for management to analyze the information it receives.

Audit Trail Management (Section 61.7 of the Directive)

91. Audit trail files are usually large and are challenging to read. They are created in a variety of systems and are sometimes difficult to manage and correlate. SIEM (Security Information and Event Management) systems, for example, can provide a means of collecting, aggregating, analyzing, and correlating information from separate systems and applications.

    Audit trail analysis enables the banking corporation to identify problems, investigate suspicious activity, understand the normal activity of the information technology (IT) system in terms of performance and capacity, and improve it.

    The challenge facing any banking corporation is to balance all of the following components that make up the audit trail: the amount of data collected, the availability of storage space and capacity, the ability to analyze data, and the ability to respond to the conclusions that emerge from this analysis.

    The higher the risk assessment, the more in-depth analysis of the logs is required, more frequently and by more sophisticated means.

Disposal of data and media (Article 61.8 of the Directive)

92. Data deletion and disposal or transferring of media and equipment are processes that are jointly carried out by a number of functions within the banking corporation, including operations, information security the Chief Cyber Defense and Information Security Officer (CISO), and third-party management, if applicable. The procedures will define the method of disposal or destruction according to the type of data to be deleted. For example, a banking corporation may choose to physically destroy media that contains sensitive customer data in order to prevent the recovery of this data and its improper use.

    The process will also determine which data is not required for deletion.

93. For the avoidance of doubt, the meaning of the transfer of media and equipment in this section is from Entity A to Entity B, whether in the banking corporation or outside it (for example, the provision of a printer as a donation), and does not mean the removal and use of media and equipment by an employee of the

banking corporation outside the walls of the banking corporation, for example in his home. (Regarding the removal and use of physical media of the type of printouts outside the walls of the banking corporation by an employee of the banking corporation – see Section 134 of the directive).

94. A banking corporation will consider using data erasure techniques even when the media is transferred between different departments within the banking corporation, since not all departments in the banking corporation are usually required to access the sensitive or classified information on the same media. For example, sometimes the computer of a departed employee is reused, so if the employee who left was granted access to sensitive customer data, it must be deleted from that employee's computer before it is transferred to another employee in another department of the banking corporation.

95. A banking corporation that engages with a third party shall make sure to update in its contract arrangements for the deletion of the banking corporation's data stored with it, including with a party that engages with that third party for the purpose of executing the contents of the engagement for the banking corporation. The arrangements will be determined according to the criticality and sensitivity of the data.

    Section 30(a) of Directive 362 requires the deletion of the banking corporation's information only from the systems of a substantial cloud computing service provider. Therefore, there may be cases in which the deletion arrangements required in each of the directives will be different. In such a case, the stricter of the two provisions will apply. For example, it is possible that a significant cloud computing service provider will be required to delete all data stored by it in accordance with Directive 362, even though some of the data is defined as non-sensitive, whereas according to this directive, the banking corporation is not obligated to delete data that is not defined as sensitive. In such a case, the deletion obligation will apply.

    It should be noted that in accordance with Section 23(g)(3) of Directive 359A, in the case of a third party that is also defined as a "service provider" in accordance with Directive 359A, the banking corporation must consider including the issue of

the manner of returning the information to the banking corporation within the outsourcing agreement.

Service and Support Processes (Section 62 of the Directive)

96. The following are examples of additional service and support processes for the "Incident and Problem Management" processes presented in the section as an example:

96.1. Help-Desk Services – In this process, the Help-Desk provides technical assistance, assistance in solving problems related to software, hardware or networks, and assistance in the event of incidents and problems – to the employees of the banking corporation and its customers.

96.2. Operational support – IT employees provide operational processes that support the banking corporation's lines of business (for example: running a job on the central computer). Since the management of the business line does not have the appropriate knowledge to examine these processes, the management of the banking corporation must lead, for example:

96.2.1. Processes to ensure the completeness and accuracy of data ingestion into systems and its processing..

96.2.2. Controls to ensure that data ingestion from external parties and its processing are conducted in accordance with the banking corporation's information security and cyber defense policies..

96.2.3. Controls that ensure that data has not been damaged during its intake or as a result of failures in its processing.

96.2.4. Mechanisms for reporting malfunctions in data intake and processing.

Monitoring, Evaluation and Reporting Processes (Section 63 of the Directive)

97. Monitoring, evaluation and reporting processes support the proactive management of the information technology system and help guide the banking corporation to achieve its current goals and plans for the future, such as: growth, mergers or expansion of the business line.

The following are examples of types of reports on the activity of the Information Technology Division:

97.1. Report on capacity utilization.

97.2. Reports on system availability, system response times, and processing times.

97.3. Integrity and accuracy of transactions.

97.4. Comparing an agreed level of service (SLA) against actual performance.

97.5. Use key performance indicators (KPIs) that allow you to determine how well the implemented process helps achieve goals.

Principles for the Proper Implementation of the Information Technology Planning and Investment Process (Section 64.1.4)

98. The technological resources include, inter alia, the following components, and the banking corporation is required to ensure their compatibility with the current and expected needs of the banking corporation:

98.1. Infrastructure – for example: electricity, communications, network architecture and suitable facilities.

98.2. Hardware – for example: central computer, servers, networks, desktop computers, mobile devices, storage devices.

98.3. Operating software – for example: operating systems, compilers, components designed to help the equipment and operating software function properly.

98.4. Apps including, applications, and systems.

98.5. Skilled workers.

99. Planning is a process in which the banking corporation prepares for future activities by defining objectives and the strategy for achieving them. Future activities include, but are not limited to, the introduction of a new product or service, planned mergers and acquisitions, or preparations for the cessation of support for an information system. Information technology (IT) is an integral part of the banking corporation's business activity. Therefore, a banking corporation is required to incorporate considerations of resource allocation and technology investments as part of the overall business planning process. Significant investments in technology have long-term implications for the performance of products and services offered by the banking corporation and on the proposition of new ones.

100. The board of directors, senior management and employees will participate in the proper planning process. The Board of Directors will challenge the senior management regarding the effectiveness of the planning process when approving

the information technology policy as detailed in Section 15 of the Directive, and senior management will formulate the information technology policy and an annual and multi-year work plan in the field of information technology as stated in Sections 19.3 and 19.4 of the Directive.

101. The planning process shall be adapted on an ongoing basis to new risks facing the banking corporation and the opportunities it faces, while maximizing the contribution of the information technology system to it.

Engagement with third parties in the planning process (Section 64.2 of the Directive)

102. As part of the checks to ensure that the third party can continue to support the banking corporation's plans, the banking corporation may review the third party's website, relevant press clippings, and periodic updates from the third party or any other information source, in order to be updated with the third party's activities, changes in its strategy and the services it provides, its future plans, and its other future liabilities (existing or future). A third party's planning to change the nature of its activity or personnel, and various issues related to information security or the service it provides.

Chapter F - Project Management and Change Management

General (Sections 65-99 of the Directive)

103. The Directive defines the desired outcomes of the project management and change management processes and the principles that the banking corporation is required to implement in order to achieve these outcomes. The Directive does not define specific methods by which the products can be achieved, and the best way to implement the principles detailed in the Directive is up to the decision of the banking corporation. The Directive is appropriate for accepted project management and change management concepts and methods and is technology neutral.

Framework for Information Technology Project Management (Section 65 of the Directive)

104. A proper process for managing information technology projects is a key factor in proper management of the information technology system and includes knowledge, expertise, tools, and techniques to achieve project goals. The operational complexity of the banking corporation dictates the level of formality of project management practices. The banking corporation's ability to manage projects affects its ability to adapt to changes in the business environment and its ability to meet the strategic goals it has set for itself.

105. The work framework for IT project management will define, at a minimum, roles, areas of responsibility, authorities, and reporting lines, and it will distinguish between different types of projects according to the criticality and sensitivity of the information asset relevant to the project, and in accordance with the additional characteristics detailed in the section. For example, an innovative project by its very nature will require more managerial attention, and the banking corporation will be required to determine a suitable framework.

Policy for the Management of Information Technology Projects (Section 67 of the Directive)

106. The policy for managing information technology projects is part of the information technology management policy of the banking corporation.

107. The section requires that the policy relate to the manner in which the topics detailed therein are implemented in accordance with the different types of projects. For example, the policy will determine what type of project will be required to determine key milestones.

Identification, Assessment and Minimization of Risks in Information Technology Projects (Section 71 of the Directive)

108. The realization of risks in the project can negatively affect the timetables for its delivery, its budget, and its quality. Accordingly, the banking corporation is required to monitor the risks arising from the project.

Due diligence when acquiring a system (Section 75 of the Directive)

109. In accordance with the provisions of Section 5 of the Directive, in the case of a third party that is also defined as a "Service Provider" in accordance with Directive 359A, the level of due diligence that will be carried out will be in accordance with

the criticality and sensitivity of the information asset, and in addition, it will also be required to comply with the provisions of Sections 18-21 of Directive 359A.

System development and implementation (Sections 79-83 of the Directive)

110. For the avoidance of doubt, this sections also relates to a case in which the banking corporation has purchased a system and it wishes to implement it or wishes to implement a system that it purchased and part of which was developed by it.

Measures to Minimize the Risk of Change (Section 79 of the Directive)

111. A banking corporation is required to ensure that steps have been taken to prevent human error and to prevent actions deliberately harming the system, during the process of development and implementation of the system in the production environment.

Access as needed (Section 81 of the Directive)

112. In granting access on a need-based basis, permissions are granted only in time access, as opposed to a process in which permanent permissions are granted in a one-time process**.**

Life Cycle of System Development and Implementation (Section 82 of the Directive)

113. The System Development Life Cycle (SDLC) is a conceptual model that describes the stages involved in a system development project, from the initial feasibility stage to the maintenance stage. SDLC can be relevant to information assets such as hardware and software. Every hardware, software, and system will go through a development process, which can be thought of as a series of repetitive processes with a large number of steps. SDLC is used as a rigid structure and framework for defining the stages involved in the system development process. SDLC methodologies, include Waterfall, Spiral, and Agile. SDLC methodology focuses on the following stages: initiation, requirements collection, planning, design, software development, testing, implementation, and maintenance.

API (Application Programming Interface) Development (Sections 84-91 of the Directive)

114. APIs allow a variety of applications to communicate with each other and receive and transfer data. APIs are interfaces that are available to third parties and that

provide developers programmatic access to applications or web services. A banking corporation can cooperate with fintech companies, etc., and develop APIs that will be used to transfer information or data to and from third parties. Hence, it is very important for the banking corporation to implement proper controls for the secure management of the development and operation of APIs.

For the avoidance of doubt, it is clarified that this sections details the principles of information security regarding the development and management of a secure Open API vis-à-vis third parties, both those that are considered a "third party provider" as defined in Proper Conduct of Banking Business Directive no. 368 on the subject: "Open Banking" (hereinafter: "Directive 368"), and those that are not considered a "Third Party Provider" as defined in Directive 368 and with whom the Banking Corporation chooses on its own initiative to engage in such an interface (even though it is not obligated to do so by law), as part of business initiatives. It should be emphasized, however, that Sections 85-87 of the Directive will not apply in the case of a third party to whom Directive 368 applies.

Deployment of Emergency Changes to Production (Section 97 of the Directive)

115. As a rule, emergency changes must also be made in accordance with the normal change process customary in the banking corporation. However, there may be urgent changes or emergency changes, such as a security patch of high importance and high priority, which are changes that need to be implemented quickly, and for which the normal change management process stated in Section 61.4 of the Directive and under this subject ("Change Management") cannot be applied. Such changes will be made in very exceptional cases.

Part IV – Information Security and Cyber Defense Risk Management

Chapter G – Information Security

Assessing the adequacy of the information security capability (Section 100 of the Directive)

116. An ongoing assessment of the adequacy of the banking corporation's information security capability can be carried out in a variety of ways for example,

by reviewing one or more of the following parameters: the adequacy of resourcing, including funding and staffing, timely access to necessary skill sets and the comprehensiveness of the control environment—preventative, detective and responsive.

Components of Information Security Capability (Section 101 of the Directive)

117. The current threat landscape faced by banking corporations, including cyber attack threats, requires unique information security capabilities beyond general information security controls. These unique information security capabilities will include, among other things, the components listed in the section.

Assessing the adequacy of a third party's information security capability (Section 102 of the Directive)

118. A banking corporation shall assess the adequacy of a third party's information security capability, inter alia in terms of the sufficiency of the resources, skills and controls assigned to it. This assessment can be carried out through a combination of a variety of tools such as: interviews, service reporting, control testing, and independent assurance assessments.

Information Security and Cyber Defense Management Framework (Section 103 of the Directive)

119. The section states that a framework for managing the information security and cyber defense of the banking corporation will coordinate its information security risks. This requirement is intended to emphasize the Banking Supervision Department's expectation that the information security and cyber defense framework will be updated in accordance with changes in the outline of information security risks facing the banking corporation.

120. Instructions to the customers of the banking corporation regarding information security, as required in this section, can be given through technological restrictions, for example, requiring the customer to set an X-character password .

High-level core principles underlying the framework for managing information security and cyber defense (Section 105 of the Directive)

121. The framework for managing information security and cyber defense would be informed by a set of information security principles that will guide decision makers

regarding information security. The implementation of the minimum principles specified in Section 23 shall establish an adequate foundation for the banking corporation's information security and cyber defense framework, and shall contribute to the reduction of the attack surface (i.e., the aggregate of activities and system resources externally exposed):

Defense in Depth (Section 105.1 of the Directive)

122. Implementing defense in depth by implementing multi-layer defense can significantly strengthen the overall security of business processes, information systems, banking products and services, as well as be effective in protecting sensitive customer information, preventing identity theft, and preventing losses due to unauthorized use.

Least Privilege and Need to Know (Section 105.2 of the Directive)

123. Applying this principle may reduce the number of attack vectors (external interfaces of the system that together constitute the attack surface) that can be exploited to compromise the information security of the banking corporation.

Timely detection of Information security Incidents (Section 105.3 of the Directive)

124. The identification of an information security incident should be in a timely manner that will allow the impact of the damage to information security to be minimized.

Preventing unauthorized access or other compromise of information security when an error occurs (Section 105.7)

125. The banking corporation must prevent a situation in which an error, whether caused intentionally or unintentionally, will cause a breach of information security. For example, a server received a request with unexpected information (e.g., a blank username), and as a result, exposed details that it should not reveal.

Never Trust Always Verify (Section 105.8 of the Directive)

126. The banking corporation must pay special attention to unrecognized entities before relying on them, including taking extreme caution in dealing with unrecognized internal and external information assets, because the level of information security controls in these assets is unknown and may not be sufficient.

Segregation of Duties (Section 105.9 of the Directive)

127. Applying this principle reduces the potential for the corporation's information security to be compromised by a single employee.

Information Collection (Section 105.13.2 of the Directive)

128. The principle of situational awareness deals with the perception of the cyber security situation of the banking corporation, in the current period of time, in the face of threats, carrying out comprehensive monitoring of the internal and external environment of the banking corporation in order to identify weaknesses and/or threats and/or information security incidents and/or indicators of their existence, using various identification capabilities - for example: pattern analysis, anomaly detection, big data analysis - and prioritization of events considering the level of risk and potential damage inherent in them, as a basis for making operative decisions.

Information Security and Cyber defense Policy (Sections 106-107 of the Directive)

129. It is clarified that the provisions of these sections do not derogate from the obligation regarding the management and updating of the database definitions document, as set forth in Regulation 2 of the "Privacy Protection Regulations (Information Security), 5777-2017".

130. The policy should address the issues specified in Section 106 of the Directive. If necessary, it is possible to expand on these issues by referring to an appropriate document in which the issue will be regulated in more detail.

Chapter H: Implementation of Information Security Controls

General (Sections 108-110 of the Directive)

131. As stated in Section 9 of the Directive, the information security risk management process, including the implementation stage of controls against those risks, must be in accordance with the operational risk management principles detailed in Directive no. 350 and the general risk management principles detailed in Directive no. 310. In addition, in the process of implementing information security controls, additional emphases will be applied as detailed in this chapter.

To protect the information assets and further to the risk assessment process detailed in Chapter G of the Directive a banking corporation is required to

implement information security controls that correspond, inter alia, to the level of criticality and sensitivity of the information asset, and the stage of the life cycle in which the information asset resides. The banking corporation must ensure that the information security controls remain effective at every stage of the information asset's life cycle.

132. Mapping the information security controls implemented or planned to be implemented by a third party can be carried out through a combination of various tools such as interviews, surveys, control tests, approvals, and opinions of independent parties.

Implementation of information security controls by a third party (Sections 109-110 of the Directive)

133. The requirements in these sections are requirements for the implementation of information security controls on information assets managed by a third party and must be carried out before or during the engagement with him. Regarding the requirement to evaluate the effectiveness of the controls implemented on information assets managed by a third party – see Chapter I of the Directive "Assessing the Effectiveness of Information Security Controls".

Identifying, assessment, and implementation of controls commensurate with information security vulnerabilities and threats (Section 111 of the Directive)

134. The process of identifying, assessing, and implementing information security controls should be ongoing and carried out, among other things, in accordance with internal and external changes, including business, organizational, and technological changes.

135. A banking corporation is required to have a full understanding of the information assets on which its business activity rests, and to focus on those information assets, which in the event of an information security incident will have the greatest impact on it. At the same time, "the strength of a chain is determined by the strength of its weakest link", and therefore the section states that the banking corporation must identify and assess vulnerabilities and threats with respect to information assets through which critical and sensitive information assets can be compromised.

136. Remediation activities are proactive actions undertaken to identify and eradicate the threat. These activities are a central component of the banking corporation's information security and cyber defense strategy, and they help the banking corporation respond to information security threats, for example: in cyber attacks – contain the damage, and eliminate the threat as a whole.

137. The threat and vulnerability landscape of the banking corporation can be derived, inter alia, from the following information: mapping of relevant threat factors with respect to motivation and capabilities; techniques, tactics, scenarios and attack tools; Vulnerabilities, system settings, or vulnerabilities that could be exploited for attacks; actions taken in the past in response to an attack, attacks that occurred in the past (at the banking corporation and/or in its operational environment); methods and indicators for detecting and identifying attacks; methods of coping with attacks.

Information Security Controls in the Information Asset Life Cycle (Sections 112-115)

138. The sections address the life cycle of the information asset, which is broader than the software development life cycle. The stages of the life cycle of the information asset include: planning and design, acquisition, implementation, decommissioning, and destruction.

Vulnerability Management Controls (Section 114.7 of the Directive)

139. Vulnerability management is a continuous process in which the banking corporation obtains information about new vulnerabilities, analyzes it, and takes action accordingly, including addressing them while reducing the window of time for them to be exploited by a hostile party. Vulnerability management also includes a patch management process.

In accordance with the general requirement in Section 15(c) of Directive 310, under which an appropriate internal control environment must be established and formalized in clear procedures uopn which the banking corporation's risk management framework is based, the banking corporation is required, inter alia,

to establish procedures for the continuous updating of vulnerabilities relating to information assets.

Capacity and Performance Management Controls (Section 114.11 of the Directive)

140. A process for capacity and performance management involves operational and technological aspects (see Section 61.6 of the Directive – "Capacity and Performance Management") that affect the availability of the information asset. At the same time, the process of capacity and performance management can also be exposed to purely information security risks. For example, a DDoS attack incident in which a hostile party causes the server to crash by sending multiple requests to it.

Identity and Logical Access Management Controls (sections 116-120 of the Directive)

141. For the avoidance of doubt, the provisions of sections 117-119 of the Directive do not detract from the banking corporation's obligation to comply with Section 14(c) of the Privacy Protection (Information Security) Regulations, 5777 – 2017, with the exception of the end of Section 14(c) of the Privacy Protection Regulations (Information Security), 5777 – 2017, which will not apply to customers' access to information about them.

Establishing Controls for Identity Management and Logical Access Management (section 116.1 of the Directive)

142. Access permissions are typically granted to individuals, designated system accounts, and information assets such as system and software services.

A banking corporation is required to establish controls for identity management and logical access management for each party that has access to the information asset. For the avoidance of doubt, it is clarified that this also refers to a third party who has access to the information asset.

Exceptions (Section 116.2 of the Directive)

143. An example of an exceptional situation in which it is not possible to determine personal means of identification and authentication is computer operators working in shifts, where the computer is operating continuously, and the implementation of

personal identification and authentication mechanisms would require a complex process of replacing users that may disrupt operational continuity.

Strength of Identification and Authentication Mechanisms (Section 119 of the Directive)

144. Accepted techniques for increasing the robustness of identification and authentication mechanisms include, inter alia, the use of strong passwords (e.g., parameters affecting password strength, such as length, complexity, restrictions on reuse, and high frequency of changes), encryption techniques, increasing the number of required authentication factors (multi-factor authentication), as well as the use of technologies that combine identification and authentication, data confidentiality and integrity, and non-repudiation, for example, PKI (Public Key Infrastructure) devices (use of public and private keys).

For the avoidance of doubt, strong authentication is not necessarily within the meaning of the term "strong authentication element" in the Payment Services Law, 5779 – 2019.

Minimizing exposure to severe yet plausible scenarios (Section 121 of the Directive)

145. Examining a scenario in which malware penetrates the system and compromises encrypted information within it, its storage components, including the banking corporation's networks and cloud storage arrangements, can serve an example for the examination of a low-probability scenario with a significant impact as required in this section. This type of attack can illustrate, for example, the importance of protecting the backup environment in the event that the production environment is compromised. Such protection may be achieved, inter alia, through network segregation, strong access controls, and restrictions on network traffic.

Physical Access and Environmental Controls (Section 122 of the Directive)

146. The lack of physical and environmental access controls can compromise the effectiveness of other information security controls. A banking corporation is required to implement these controls in its premises and in the outsourcing facilities it uses.

Security Testing to Identify Vulnerabilities (Section 124.1 of the Directive)

147. The section states that the banking corporation must set checkpoints throughout the change process in order to ensure that information security and cyber defense requirements are identified, planned, built, and examined so that the level of information security continues to support the banking corporation's business objectives. The nature of the examination will be determined according to the level of criticality and sensitivity of the information asset affected by the change (and not only the information asset in which the change is made) and can range from a comparison of similar changes made to an examination itself.

Development and approval of changes in another environment (Section 124.3 of the Directive)

148. The banking corporation is required to develop and test changes (including planned, urgent, and emergency changes to software, hardware, and data) in an environment separate from the production environment. For this purpose, consideration should be given to establishing a number of environments that reflect the different stages in the development and testing of the changes.

Submission of a change as an emergency response for which the normal change management process cannot be applied—see Section 97 of the directive.

Use of real data, after it has been desensitized, as part of development and testing (section 124.5 of the Directive)

149. The section states that, where necessary, real data may be used after it has been desensitized.

Minimizing changes involved in creating information security vulnerabilities that cannot be addressed (Article 124.6 of the Directive)

150. Sometimes it is necessary to make some kind of change in production, but it is known that this change also entails the creation of information security vulnerabilities for the banking corporation that cannot be addressed at the time. In such a situation, during the ongoing operation, of course, the change cannot be introduced into production, until the information security vulnerability has not been addressed. At the same time, there may be cases in which the risk assessment from not introducing the change will outweigh the risk assessment from the introduction of the change while applying compensatory controls. In such cases, it

is possible to introduce the change into production, provided that the prior consent of the appropriate authority is obtained and with the implementation of compensatory controls as much as possible.

Such a situation, in which the change includes information security vulnerabilities knowingly, usually occurs in old systems or technologies used by the banking corporation. The Banking Supervision Department believes that the need for prior approval of changes that knowingly create information security vulnerabilities will reduce such phenomena to the required minimum, and encourage the implementation of compensatory controls.

Controls over means that potentially expose sensitive information (Article 126)

151. This section deals with the access controls required to prevent individuals with authorized access from removing, copying, distributing, or otherwise disclosing information that has been defined as sensitive, in those places where there is a risk of data leakage.

The following are examples of means that, when improperly used, may allow unauthorized disclosure of sensitive information: mobile devices (laptops, tablets, mobile phones, etc.), mobile storage devices, means of electronic transmission (email, instant messaging software, etc.), and means of data transmission (printers, telephony, video conferencing equipment, etc.).

Principles for the Use of Cryptographic Techniques (Section 127.1-127.4 of the Directive)

152. Cryptographic techniques are methods used to encrypt data, confirm its authenticity, and verify its integrity.

A banking corporation is required to use cryptographic techniques for the purpose of controlling access to its data in motion and its data at rest and to the media through which network traffic is transmitted, in accordance with an appropriate risk assessment that will take into account, inter alia, the nature of the activity under consideration (for example, the transfer of data over an medium that is not under the exclusive control of the banking corporation), and the degree of criticality and sensitivity of the data.

Notwithstanding the above, in any case of storing data classified by the banking corporation at a high level of criticality and at a high level of sensitivity outside the banking corporation's internal network, and in any case of data transfer at all on a public network or on a network where the banking corporation cannot enforce its information security and cyber defense policies, the banking corporation is required to make, at a minimum, the use of accepted encryption techniques.

It should be emphasized that the encryption of the network transmission medium does not necessarily make the encryption of the data transmitted through it redundant. Conversely, data encryption does not necessarily make the encryption of the network traffic medium redundant. Accordingly, there may be cases in which encryption of both the data and the medium of traffic will be required.

The strength of the cryptographic technique used will be determined in accordance with a risk assessment that will take into account, inter alia, the degree of criticality and sensitivity of the data, the nature of the activity, and additional controls.

Requirements and Exceptions Regarding Encryption in Directives 362 and 367 (Section 127.5 of the Directive)

153. The banking corporation must implement the provisions of subsection 127.3 – 127.1 of this directive, with respect to all of its data. However, there are cases in which the Banking Supervision Department has found it appropriate to introduce arrangements that differ from the requirements specified in this directive, and these arrangements will continue to apply notwithstanding what is stated in this directive. For example:

153.1. Section 63 of Directive 367 – A banking corporation that transmits information about its customers over external networks, including the Internet, is required to use an encryption algorithm in order to protect such information while it is transmitted.

153.2. Section 63 of Directive 367 – A banking corporation that transmits information about its customers over the telephony network – is not obligated to encrypt this information.

153.3. Section 33 of Directive 362 – A banking corporation that transmits information over communication media to a cloud computing service provider shall encrypt it in transit as well as at rest. In cases where it is difficult for the banking corporation to encrypt all such information, at a minimum it shall encrypt data classified by it as sensitive, or data whose disclosure may harm the banking corporation and its customers.

154. It should be emphasized that the requirements and exceptions regarding encryption detailed in Directive 367 are relevant only to customer information transmitted as part of the provision of banking services through communication banking channels, as defined in Section 8 of Directive 367. Accordingly, customer data that is not transmitted as part of services provided through communication banking channels as described above, and does not fall within the scope of the application of Section 33 of Directive 362 is required to be encrypted in accordance with the provisions of Sections 127.1 – 127.3 of this Directive.

Controls for the proper management of cryptographic keys (Section 127.6 of the Directive)

155. Proper management of cryptographic keys ensures that controls are implemented to reduce the risk of their exposure. Example controls:

155.1. Use physical and logical protection of devices and environments used to store and generate cryptographic keys, generate customer passwords, and perform encryption and decryption operations n.

155.2. The use of cryptographic methods to maintain the confidentiality of the cryptographic keys.

155.3. Periodic replacement of the cryptographic keys according to the risk.

155.4. Clear procedures for the process of revocation of cryptographic keys.

155.5. Implementing techniques to detect any unconfirmed exchange attempts of the cryptographic keys.

Lifecycle Controls on Technological Solutions for Information Security (Section 129 of the Directive)

156. The section stipulates that the level of application of lifecycle controls on technological solutions will be adjusted to the level of reliance of the banking

corporation on the technological solution in protecting its information assets, so that the higher the reliance, the more closely the lifecycle controls for that technological solution will be implemented.

157. The section states that the lifecycle controls on information security technological solutions shall include measures that provide warning if the information security technological solutions are not working properly, consistent with the requirement of the provision in section 114.13, to include controls that continuously verify the activity of the implemented information security controls (Continuous Control Monitoring).

Development by End Users – Processes for Identifying and Assessing Exposure to Risk (Section 130.1 of the Directive)

158. The technologies that exist today allow end users to develop and configure software for the purpose of automating ongoing business processes or for simplifying decision-making processes (e.g., using spreadsheets, local databases). Such cases in which the IT system is not involved are also called shadow IT. The risk, among other things, is that the lifecycle controls implemented in the banking corporation will not be adapted for such cases, and as a result, it will be possible to access a lot of information classified as sensitive from uncontrolled environments.

Legacy Systems (Section 131 of the Directive)

159. Information assets that were implemented prior to the establishment of the information security and cyber defense framework, are required to comply with the information security and cyber defense principles and requirements of that framework. If it is not possible to apply the aforementioned principles and requirements to those information assets, the banking corporation must consider replacing them or addressing them in accordance with the policy for deviations from the framework for managing information security and cyber defense that it has established in this regard.

Emerging Technologies (Section 132 of the Directive)

160. Section 132.1 of the Directive deals with the introduction of emerging technologies in the production environment, while Section 132.2 of the Directive addresses the examination of emerging technologies (which do not meet the conditions specified in Article 132.1 of the Directive) in a designated test environment or in a designated segregated production environment (a "sandbox").

In the context of examining emerging technologies in a designated experimental environment or in a designated production environment (section 132.2 of the Directive), attention should be paid to the Banking Supervision Department's letter No. H-390 dated June 23, 2019 on the subject: "Encouraging Innovation in Banks and Acquirers".

Telework (Sections 133-134 of the Directive)

161. As stated, the term "information assets" also refers to printouts, whether the printout is located at the offices of the banking corporation or whether the printout was issued by an employee, including a contractor who is managed by the banking corporation or temporary employee, for the purpose of working at his home or at any other location outside the banking corporation's premises.

In addition, since a printout is a type of document, the guidelines of the Proper Conduct of Banking Management Directive No. 356 on the subject: "Issuance of Documents from the Offices of Banking Corporations" will also apply to it in accordance with the matter.

The Banking Corporation's Connectivity to Public Networks (Section 135 of the Directive)

162. For the avoidance of doubt, the Internet is public network.

163. The following is an example of mechanisms required under this section for the purpose of protecting the online presence of the banking corporation: measures to detect impersonation of its website, and providing customer with appropriate tools to verify the authenticity of the website.

164. Among the risks involved in the banking corporation's activity on social networks are risks in the following areas: customer identification and authentication (including impersonation using information obtained from the social networks),

information disclosure, fraud, and malware penetration through social networks, etc.

Chapter I - Assessing the Effectiveness of Information Security Controls

Mapping and Testing Information Security Controls (Section 136 of the Directive)

165. The banking corporation is required to map all information security controls implemented across the organization, and to establish an on doing testing program that validates the effectiveness of their design, implementation, and operation.

"Systematic Testing Program" – a program that is structured and executed according to a predefined methodology or a sequence established by the banking corporation.

Frequency and Scope of Testing (Section 137.1 of the Directive)

166. The frequency and scope of the checks will be designed to ensure that a sufficient set of the banking corporation's information security controls are tested at least once a year, so that the banking corporation can reasonably ensure that these controls remain effective.

In addition, when determining the frequency and scope as aforesaid, the banking corporation will take into account, inter alia, the degree of criticality and sensitivity of the information asset for which the controls are intended, as well as the possible consequences of the information security incident affecting the information asset for which the controls are intended.

In any case, each information security control shall be reviewed at least once every three years.

Testing of the effectiveness of the controls (Section 137.2 of the Directive)

167. In addition to conducting tests in accordance with the testing program, the banking corporation will conduct tests on the effectiveness of information security controls, inter alia, in any case of material changes in the information asset, in the technological environment in which the banking corporation operates, or due to

new vulnerabilities and threats that have been discovered, inter alia, due to information security incidents that have occurred.

Controls related to information assets exposed to environments where the banking corporation cannot enforce its information security and cyber defense **policy (Section 137.3 of the Directive)**

168. Environments in which the banking corporation cannot enforce its information security and cyber defense policy are, for example, an environment that is exposed to the Internet, and an environment that provides connectivity to third parties and customers.

Defining the types of tests Section 138.1 of the Directive)

169. The banking corporation has a wide range of tools for testing information security controls, and in each test it must adapt the appropriate tool to the control being tested, taking into account the accepted practice at the time. The following are examples of control objectives, information security controls that are suitable for these purposes, and tools by which their effectiveness can be tested and assessed:

Control objective	Examples of controls and practices	Examples of tools that can be used to test and assess the control
Limit access to what has been authorized based on the user's role and the principle of least privilege	IAM-Identity and Access Management, User Identification and Authentication, Physical Security, Employee Awareness, and Employee Training	Social Engineering Tests
User authentication at a level that matches the sensitivity of the information asset they wish to access	Password Policies, System authentication controls	Audits of user access according to the sensitivity of the information asset.

Control objective	Examples of controls and practices	Examples of tools that can be used to test and assess the control
Protect networks from unauthorized network traffic	Firewalls, Routers, Network segmentation	Penetration Tests
Protect systems from malicious attacks	Use of anti-malware, email and web filtering	Malware test samples, configuration tests.
Protect system to system communication, including exchange of data, from unauthorized access and use	Encryption, Key Management	Key management review
Timely detection of unauthorized access and use	Logs, SIEM (Security Information and Event Management), Security Cameras, Intrusion Detection System (IDS), Integrity change detection solutions, Event analysis and escalation Procedures	Controlled penetration tests, including more advanced techniques such as "red team" tests.
Implement Secure Software	Secure software development, secure software procurement and deployment practices.	Design reviews, penetration tests, code review and scanning, Network traffic analysis, fault testing, fuzzing
Orderly response to information security incidents	Information security incident response playbook, crisis	Holding table top exercises—role-playing

Control objective	Examples of controls and practices	Examples of tools that can be used to test and assess the control
	management, business continuity plan (BCP)	games in preparation for an emergency.
System resilience to handle failure of individual components	Active-Active or Active-Passive solutions deployed, sandboxed solutions (a gated environment that allows the program to access only certain resources and that keeps the issues that occurred in that environment from affecting the rest of the system environments), Zero Trust architecture	Performing Chaos monkey testing, architecture review, fault testing, failover testing.
Recovery under all plausible scenarios	Recovery Plan, Arrangements and Tests. Controls to prevent unauthorized access to the backup environment.	Technical recovery tests, Backup environment penetration test
Implementation controls that minimize the risk of new vulnerabilities as a result of changes in the system, the systems are	Secure software development, change controls, systems hardening,	Change control review, code scanning, architecture review, automated software tests in which an unexpected

Control objective	Examples of controls and practices	Examples of tools that can be used to test and assess the control
developed so that the principles of information security and cyber defense are integrated into them already at the system design stage (Secure by Design)		value is inserted into the system (fuzzing)
Timely identification and remediation of new vulnerabilities	Patch Management, Configuration Management	Scanning for vulnerabilities, penetration testing
Timely identification and remediation of new threats	Threat intelligence, Information Security and Cyber Defense Strategy	Independent capability review

The banking corporation's reliance on tests to assess the effectiveness of third-party controls over information assets managed by it (section 140)

170. The evaluation of the effectiveness of controls over information assets managed by a third party should be carried out in accordance with the principles according to which the effectiveness of the controls in the banking corporation is evaluated. To the extent that the banking corporation assesses that there are gaps in the application of such principles by a third party, it must examine the continued use of its services.

Part E – Incident Management

Chapter J – Monitoring Information Technology

General (Sections 141-143 of the Directive)

171. Some of the technological failure incidents and information security incidents (hereinafter: "incidents") can be prevented or at least detected at an early stage, inter alia, by early identification of suspicious patterns and anomalies in the activity of both the Banking corporation's systems and customers.

For example, identifying a server that reaches the utilization of 80 percent of its memory can prevent the system from crashing unexpectedly. Thus, for example, identifying a very large number of requests to the server at a given time beyond normal level or identifying suspicious customer activity, can indicate the beginning of a cyberattack on the organization.

Accordingly, the banking corporation is required to establish policy and procedures for identifying emerging or anomalous problems in order to proactively prevent them from developing into such incidents. The policies and procedures will define ongoing monitoring processes that will operate throughout the week, 24 hours a day, and that will monitor, among other things, the activity and performance of the systems – in terms of control and oversight, business activity, including transactions, and the activities of relevant internal parties (such as personnel in the business functions and administrative functions of the information technology system) and external, as well as monitor potential internal and external threats.

172. As part of the monitoring measures, the banking corporation is required to maintain a monitoring and control system, which will be staffed continuously (24X7X365), receive real-time reports from the various systems, including operational and business systems (monitoring and control) and various information security and cyber defense systems (such as SIEM/SOC). This system will identify indicators of the occurrence of technological failure and information security incidents, and initiate reporting and response activities if necessary.

173. Examples for monitoring controls that the banking corporation may consider implementing to fulfill the requirements of the chapter:

- Creating an activity profile for networks and users, along with logging and alerting mechanisms, for the purpose of identifying anomalous activity.
- Scanning for detection of unauthorized network hardware or software or unapproved configuration changes.
- Implementing sensors that detect exceeding a predefined threshold while providing appropriate alerts.
- Logging and alerting for access to sensitive information or unsuccessful access attempts.
- Increased monitoring of users with special access privileges (e.g., administrators).

Chapter K - Incidents and Problems management

Implementation of an incident management process (Section 144 of the Directive)

174. An incident occurs when there is a technological failure incident or an information security incident as defined in Section 11 of the Directive.

175. The incident management process is designed to achieve two main goals:

175.1. Monitoring the incident as it occurs in order to reduce its impact and resume the banking corporation's activity quickly.

175.2. Documenting the incident for the purpose of learning and drawing lessons.

The Incidents and Problems Management Framework (Section 146 of the Directive)

Procedures for managing problems (Section 146.5 of the Directive)

176. Problem management is a process designed to achieve a root solution to recurring and complex problems.

Reporting of incidents with a potentially high adverse impact on critical and sensitive information assets (Section 146.6.1 of the Directive)

177. Certain incidents have the potential to develop into a crisis. A banking corporation will update senior management, IT management, and other relevant internal entities on the status of these incidents so that decisions regarding mitigating the impact of the incident can be made quickly, such as a decision to activate the disaster recovery plan.

Reporting when a significant incident occurs (Section 146.6.2 of the Directive)

178. While Section 146.6.1 of the Directive deals with significant incidents that have occurred and have the potential to have a high adverse impact on critical and sensitive information assets of the banking corporation, this section deals with such incidents that have the potential to have a high adverse impact on critical and sensitive information assets that have been realized in practice.

It is clarified that there may be technological failure incidents or information security incidents that will be defined by the banking corporation as significant and in the event of which the banking corporation has decided that an immediate report should be submitted to the Board of Directors, but they will not be obligated to report to the Banking Supervision Department in accordance with the reporting criteria detailed in Directive 366.

For the avoidance of doubt, a significant technological failure incident and a significant information security incident in this section are not necessarily the incidents that are the subject of Section 41.7 of this Directive.

Response Plans (Section 146.7 of the Directive)

179. The level of detail of response plans should be such that it minimizes the requirements for decision-making during an incident and provides clarity regarding the roles and responsibilities of each party during the occurrence of an incident.

Cooperation and Coordination with a Third Party (Section 146.10 of the Directive)

180. Response plans are required, among other things, to mitigate the impacts associated with the incident and to ensure that the service is back up and running. Response plans typically integrate with the business continuity plan. Accordingly, the section states that in the event that a banking corporation uses a third party,

it must ensure coordination between its response plans and the response plans of the third party, as well as between its response plans and the business continuity plan of the third party.

Information Security Incidents (Sections 147-152 of the Directive)

181. Information security incidents in general, and cyber attacks in particular, have unique characteristics that are expressed, among other things, in the sophisticated adversary and the evolving nature of the incident. These incidents are not always identified in time, the information about some of these incidents comes from external sources, and they usually require additional investigation in order to identify whether the information security of the banking corporation was actually compromised. Accordingly, the following are additional emphases on those detailed in Sections 144-146 of the Directive, which should be applied to such incidents.

Part F – Miscellaneous

Chapter M –Third Party Risk Management

Information Technology Risks Associated with Third-Party Arrangements (Section 155 of the Directive)

182. The management of outsourcing-related risks creates another significant aspect in the framework of the banking corporation's information technology risk management framework. Accordingly, and in addition to the outsourcing-related stability requirements detailed in Proper Conduct of Banking Business Directive no. 359A on "Outsourcing" and in Directive 362, this directive expands and adds, on a variety of topics.

The guidance on these issues was assigned to the relevant sections of the directive, so that for example, the duty of the board of directors to consider, in all of its deliberations, the aspects arising from the banking corporation's use of third parties – appears in section 18 of this directive. The appendix to the directive contains a summary of the instructions for the convenience of the reader.

Chapter N – Business Continuity Management (BCM)

General

183. This chapter focuses on the technological aspects relevant to the business continuity plan.

The requirement to build a business continuity plan appears in Directive 355.

This directive emphasizes and expands on technological issues related to business continuity, in particular regarding the Disaster Recovery Plan (DRP).

184. Some of the terms used in the chapter also appear in Directive 355. Section 156 of the Directive provides that the meaning of these terms in this Directive shall be in accordance with their meaning in Directive 355. Examples of terms: "Critical Process or Service", " RTO-Recovery Time", "Magor Operational Disruption", "Business Continuity Plan (BCP)".

Business Impact Analysis (BIA) (Section 158 of the Directive)

185. Example of appropriate design: Design with redundancy of certain critical components to prevent disruptions caused by events affecting these components.

Determination of the Business Continuity Plan (Section 160 of the Directive)

186. Prioritization for example: Performing a workaround for a critical transaction while remediation actions are being performed.

187. A banking corporation can also use the risk assessment carried out in accordance with Section 46 of the Directive, and is not obligated to use a designated risk assessment for this section.

Focus of the Disaster Recovery Plan (Section 163.1 of the Directive)

188. The disaster recovery plan will relate both to the recovery of the functioning of the critical processes and services in accordance with the service objectives set by the banking corporation (including bypassing the technological process in order to meet the service objectives), and to restoring the technological processes and information assets to their state before the operational disruption occurred.

Documentation and availability of the disaster recovery plan (Section 163.2 of the Directive)

189. A banking corporation is required to prepare for various situations in which an available and accessible response and recovery plan will be required. For example, it is possible to consider keeping a copy of the plan on documents as well, in order to maintain the availability and accessibility of the plan in the event of a failure in the technological means on which it is maintained.

Chapter O - Foreign Bank

Application of the Directive to a Foreign Bank (Section 170 of the Directive)

190. "The local information technology system, including the interfaces of this system with the bank's system abroad" is any component of the information technology system as defined in Section 11 of the Directive that is under the control of the foreign bank, including components of interfaces under the control of the foreign bank.

191. To the extent that a foreign bank believes that certain sections in this Directive are not applicable to it, it has the option of making use of Section 5 of Proper Conduct of Banking Business Directive no. 100 on the subject: "Introduction to Proper Conduct of Banking Business Directives File" (hereinafter,"Directive 100"), and to apply to the Banking Supervision Department in order to coordinate the manner in which they are implemented. The Banking Supervision Department expects that Section 5 of Directive 100 will be used only in exceptional cases.

Other Topics

Handling existing instructions and approvals

192. As of the date of the commencement of this directive, Directives no. 357 on "Information Technology Management", No. 361 on "Cyber Defense Management", no. 363 on "Supply Chain Cyber Risk Management ", and the Supervisory Letters on the following subjects will be canceled:

192.1. "Information Technology (IT) Asset Management" No. 09 LM0643 of August 24, 2009.

192.2. "Management of Key Processes in the Field of Information Technology" No. 09LM0650 of 14 September 2009.

193. Approvals issued by the Supervisor or anyone on his behalf in accordance with the Proper Conduct of Banking Business Directives that were revoked as stated above, will remain in effect. If a banking corporation holds a permit permitting activity that does not comply with the directives of this provision, it shall notify the Supervisor of Banks by the date of the commencement of the directive as detailed in section 194 below, in order to clarify its matter.

Beginning and Transitional Provisions

194. The commencement of the provisions of this Directive is 18 months from the date of its publication.

195. With respect to contracts concluded prior to the date of publication of the directive – on the date of the upcoming renewal of the contract and no later than 3.5 years from the date of commencement (and a total of 5 years), the banking corporation will adapt the contracts to the directive to the extent required.

196. A banking corporation may act in accordance with this Directive at an earlier date than the date set out in Section 194 above, provided that sections 192 and 193 above also apply to it from that date.

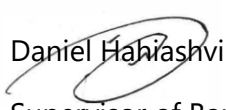
197. If a banking corporation chooses to do as stated in Section 196 above, it shall notify the Supervisor of Banks 30 days prior to such date.

Update the file

198. Attached are update pages for a Proper Conduct of Banking Business Directive file. The following are the instructions for the update:

Remove page	Insert Page
-----	364-1-57 [1] (11/24)

Sincerely,



Daniel Hahiashvili

Supervisor of Banks