# Management of IT, Information Security, and Cyber Protection Risks

# Part A – Introduction

## Chapter A – General

### Introduction

1. Information technology ("IT") currently constitutes a banking corporation's primary infrastructure for its business operations and is defined as an enabling factor in the financial sector. Accordingly, sound management of information technology is critical to a banking corporation's performance and success, and a banking corporation is required to manage IT risks as an integral part of its business operations, extending beyond purely technological considerations.

   Banking corporations increasingly rely on technology to meet the diverse challenges they face in the competitive market. A banking corporation's systems provide services to its business lines within the corporation and to the general public, and are connected to third parties that include other financial corporations (e.g., fintech companies). The role of information technology includes, inter alia, establishing appropriate connections between the infrastructures, systems, and other relevant system components in a manner that optimally supports the delivery of existing products and services and offerings of new products and services. Moreover, accurate information that is available in a timely and secured manner is critical for meeting the banking corporation's business needs and the needs of its customers.

   The rapid pace of change in technological infrastructure, the continuous innovation in banking service delivery to customers, the availability of services "anywhere, anytime," the reliance on a range of communication channels (Internet, mobile, etc.) that are also used to connect to other financial corporations, the link of the banking corporation's legacy information systems to modern and "open" computing infrastructure, as well as the growing dependence on computing and communication services rendered by third parties—all these and more challenge banking corporations' IT management, create fertile ground for growing IT risks, that include information security (IS) vulnerabilities and threats including cyber risks ("IS risks"), increase the need for a sound risk management process tailored to risks of this type, and require appropriate expertise, knowledge, and qualifications to manage the IT and its risks.

2. IT risks, which include IS risks, may pose a significant prudential threat to a banking corporation and threaten its continued existence. Accordingly, the Banking Supervision Department believes that sound management of IT risks is a fundamental component in achieving the banking corporation's strategic, corporate, and operational objectives. Therefore, a banking corporation is expected to adequately protect its information assets and assimilate an organizational culture that promotes IT and IS risk management. This Directive is designed, among other things, to ensure that the banking corporation takes steps to build adequate resilience against the materialization of IT risks through effective management of its IT array, and constantly maintaining adequate IS capability that is appropriate for addressing the IS risks that the banking corporation faces. Such measures will help the banking corporation, as much as possible, meet its financial commitments to all its stakeholders in the event that an IT risk materializes.

3. While this Directive considers cyber risk management an integral part of a banking corporation's overall IS risk management, it should be emphasized that cyber attacks have unique characteristics that the banking corporation shall consider as it ensures that the IS measures it implements to reduce IS risks are also appropriate for mitigating cyber risks. These unique characteristics include:

   3.1. The technological advances and digital transformation of recent years create increasingly fertile ground for the emergence of new vulnerabilities in a banking corporation's defense systems, which expand its attack surfaces and expose it to significant cyber risks. At the same time, cyber attacks, especially attacks targeting financial entities, have increased significantly, in terms of their scope, the range of threat actors, and the sophistication and availability of means of attack.

   3.2. Cyber attacks have distinct motives, including, but not limited to, financial crime and geopolitical circumstances. It is therefore important to understand the perceived threat landscape, relevant reference scenarios, and the defense capabilities that are accordingly required.

   3.3. Although it is important to build an early detection capability to detect cyber-attacks in real time, such attacks are difficult to identify or anticipate, and the damage they cause, especially indirect damage, is also difficult to quantify. Moreover, in extreme cases, a cyber attack may even adversely affect a banking corporation's stability. It is therefore necessary to use advanced technologies and skilled teams that know how to deal with such attacks and assess their potential damage.

   3.4. Cyber attacks may involve a banking corporation's internal or external adversaries, which may be able to respond to a banking corporation's defensive actions in real time. It is therefore important to recognize the capabilities and intentions of potential adversaries and prepare to respond accordingly.

   3.5. Cyber attacks may adversely affect a banking corporation's risk management processes and its business continuity arrangements, and in some cases may even cause the damage to spread to the banking corporation's backup systems.

   3.6. Some cyber attacks originate from entities outside the banking corporation, including third parties, as this term is defined in this Directive. In view of the potential differences between the defensive capabilities of a banking corporation and those of its linked organizations, the banking corporation shall implement appropriate controls and risk management processes to prevent such attacks spreading from its linked organizations.

   3.7. In the realm of perception, false representations of cyber-attacks may exist even if no actual attack has occurred. False representations may be produced through deception or by falsely representing unrelated malfunctions as a successful cyber-attack. The damage caused to an organization by false reports of a cyber-attack may harm the organization's reputation and may also disrupt its business operations due to the activation of response procedures for handling a suspected cyber incident.

4. The main purpose of this Directive is to support proper and effective IT management that minimizes the occurrence of incidents in which technological risks materialize and impact

the confidentiality (in information security aspects and also in the privacy aspects of the banking corporation's customers and employees), integrity, and availability of its information assets.

5. A banking corporation's information assets may be managed by third parties, either on or off the banking corporation's premises. To remove all doubt, this Directive makes no distinction between information assets managed by the banking corporation itself and those managed by a third party. This Directive applies to all the information assets of a banking corporation, including those managed by a third party, as relevant and according to the criticality and sensitivity of each information asset, and its application is not a function of the materiality of the third party that manages an information asset or of the operations performed by a third party.

   In any case where the third party is also a "service provider" as this term is defined in Proper Conduct of Banking Business Directive no. 359A on "Outsourcing" (hereinafter, "Directive 359A"), the provisions of this Directive shall apply in addition to the provisions of Directive 359A.

6. Proper implementation, appropriate use, and adequate protection of information assets may help a banking corporation identify and detect the risks to its operational resilience, increase its capability to withstand disruptions and failures, and facilitate the process of information flows in the banking corporation and reporting to relevant functions, which enables effective decision making during such disruptions and failures. The provisions of this Directive promote the security and operational resilience of the information assets in line with the provisions of the Proper Conduct of Banking Business Directives issued by the Banking Supervision Department that are relevant to operational risk management (also see Section 9 hereinafter).

7. This Directive addresses three main issues:

   7.1. IT governance within a banking corporation's overall corporate governance;

   7.2. IT risk management processes within a banking corporation's operational risk management and business continuity management;

   7.3. IS risk management processes.

8. IT risk management, including IS risk management in a banking corporation, should be based on the principles set forth in this Directive. These principles afford the flexibility that is necessary in view of the rapid pace of changes in the field of IT, IS, and cyber defense, and they are based on the recognition that every banking corporation has a unique risk profile that requires adjusting its risk management program and the manner in which the principles are implemented to the nature of its operations and its specific business needs.

9. A banking corporation's IT risk management, which includes IS risks in the banking corporation, constitutes part of its overall risk management framework, and specifically its operational risks. Therefore, this Directive is consistent with Proper Conduct of Banking Business Directive no. 310 on "Risk Management" (hereinafter, "Directive no. 310"), which defines the fundamental integrative, firm-wide principles for risk management and controls; Proper Conduct of Banking Business Directive no. 350 on "Operational Risk Management" (hereinafter, "Directive no. 350"), which defines such principles in specific reference to

operational risk, and supplements Proper Conduct of Banking Business Directive no. 355 "Business Continuity Management" (hereinafter, "Directive 355") by addressing the technological aspects of business continuity management.

**Application**

10. With respect to the application of the Directive:

10.1. This Directive applies to the following corporations as they are defined in the Banking (Licensing) Law, 5741–1981 (hereinafter, "Banking Corporation"):

10.1.1. a banking corporation;

10.1.2. a corporation as stated in Sections 11(a)(3a) and (3b);

10.1.3. a corporation as stated in Section 11(b);

10.1.4. A payment services provider with prudential importance, as defined in Section 36i.

10.2. Notwithstanding the provisions of this Directive, when a banking corporation gives access to its information assets to a third party that is a corporation in the banking group in which the banking corporation is a member, the banking corporation should act according to its risk assessment.

**Definition of terms**

11. In this Directive, the following terms shall have the meaning stated alongside them:

**Information Security** (IS) – the protection of an information asset's confidentiality, integrity and availability against unauthorized action, including access, use, disclosure, disruption, addition, deletion, or duplication, in order to ensure confidentiality, integrity and availability (CIA). Unauthorized actions also include actions that a user is authorized to perform but is prohibited from doing so by law, procedure, work practice, role definition, etc.

**IS Threat** - a circumstance or event that has the potential to exploit an information security vulnerability;

**Authentication** – confirmation of the identity of an entity that requests access;

**IS Incident** – an actual or potential compromise of information security, including a cyber-attack;

**Technological Failure Incident** - An event, incident, or result that is not expected or planned within the banking corporation's ongoing operations, and has or may have a disruptive effect on the ongoing operations of the banking corporation's IT or on the services it delivers. A technological failure incident does not include IS incidents, as this term is defined in this Directive;

**Architecture** - the manner in which the strategic design of the hardware and software infrastructure components (e.g., devices, systems, and networks) are organized and integrated to achieve and support the banking corporation's objectives;

**IS Control** - a prevention, detection, or response measure to reduce the likelihood or impact

of an information security incident;

**Data Leakage** – unauthorized disclosure of sensitive data, including disclosure resulting from human error, that results in a loss of data confidentiality;

**Authorization** – granting a user access to information assets on the basis of the banking corporation's needs and required level of information security;

**Identification** (in the context of identifying and authenticating an entity requesting access)—determination of who or what is requesting access;

**Availability** - accessibility and usability when required;

**Operational Resilience**—the ability of a banking corporation to deliver critical operations through disruption. This ability enables a banking corporation to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from, disruptive events in order to minimize their impact on the delivery of critical operations through disruption;

**Information Technology Array, Information Technology (IT)** – a banking corporation's technological infrastructure or technological architecture or services (including cloud computing services, Help Desk services, other professional services that support any point in the lifecycle of an information asset) or related resources (resources that are not considered technological infrastructure and are required for the technological infrastructure, architecture, and services, such as buildings and electricity) ;

**IS Capability** - the totality of resources, skills, and controls required to maintain proper IS operations in a changing risk environment;

**Situational Awareness** – the ability to absorb information related to threats, goals, and the environment, and to interpret it correctly and in a timely manner in order to decide on an effective course of action to accomplish the mission, to take action accordingly, and to understand how the situation changes as a result of that action, and so on and so forth;

**Sensitive Information** – information that is classified as sensitive by the banking corporation, including "data of special sensitivity" as this term is defined in the Protection of Privacy Law, 5741-1981 ("Protection of Privacy Law");

**System** – a collection of computing or communication components, together with other resources, organized for the purpose of collecting, processing, maintaining, using, sharing, or disseminating information, and that support one or more of the organization's functional objectives;

**Cyber Attack** – an incident during which an attack is conducted (even if no actual damage occurs) against the banking corporation’s digital information assets, by or on behalf of adversaries of the banking corporation, (whether external or internal);

**Damage** – an adverse outcome, including disruption/disturbance/shut down of activity, theft of an asset, gathering of intelligence, harm to reputation/public trust;

**Information Assets** - information and technology infrastructure, including data (both soft and hard copy);

**Recovery Point Objective (RPO)** – a component of a recovery objective. The maximum duration of loss of information and data for a specific process or service, as defined in the risk tolerance;

**Data at rest** – data residing in systems such as files stored on servers, databases, backup media, and storage platforms such as cloud environments, as well as data residing on endpoint devices such as notebooks, personal computers, portable storage devices, and mobile devices;

**Data in motion** – data transmitted over a public network, a network on which the banking corporation is unable to enforce its information security and cyber defense policy, or the banking corporation's private network;

**Confidentiality** – access being restricted only to those authorized;

**IS Risk –** an information security threat or vulnerability, including cyber risks;

**IT Risk** – the risk of loss due to breach of confidentiality, failure of integrity of an information asset, inappropriateness or unavailability of an information asset, or inability to change IT within a reasonable time and with reasonable costs when the environment or business requirements change. This risk also encompass IS risks;

**Cyber Risk** – the potential materialization of an IS risk through a cyber-attack;

**IS Vulnerability** - a weakness in an information asset or IS control that could be exploited to compromise information security;

**IT Project** – any project or part thereof that includes a change, replacement, removal from use, or implementation of IT systems and services. An IT project may be part of a wider IT program or part of a business change;

**Third Party** – a third party that has access to a banking corporation's information asset;

**Banking Group** – a banking corporation, a banking corporation that controls it, and corporations controlled by either;

**Criticality** (in the context of the term criticality when used with the term sensitivity) – the potential impact of loss of availability;

**Sensitivity** – the potential impact of loss of confidentiality or integrity;

**Integrity** – accuracy, reliability, and protection from unauthorized change or deletion;

**Operations** – the tactical management of information assets and the ongoing delivery of services in order to document, transfer, process, and store transactions and information that support the totality of the banking corporation's business processes;

**Technological Infrastructure** - hardware, ancillary equipment (including imaging, peripheral, input, output, and storage devices required for security and surveillance), computer-controlled peripheral equipment (including environmental controls, see Section 122 hereinafter; and physical access controls), networks and telecommunications, software, databases, firmware and similar components, as well as devices which enable IT operation and management.

## Part B – Corporate Governance and Risk Management Framework

### Chapter B – Corporate Governance

12. A banking corporation shall implement proper, effective corporate governance in the field of IT, including an appropriate framework for IT risk management and a framework for IS and cyber risk management, which, among other things, guarantees the reliability and operational resilience of its IT array and information security. Within this implementation, appropriate and clearly defined roles and areas of responsibility must be assigned to the board of directors and its committees, the senior management, relevant officers, and employees.

**Board of directors**

13. The board of directors is responsible for IT risk management in the banking corporation. Among other things, the board must ensure that the banking corporation maintains information security and other control measures in a manner commensurate with the size and extent of the risks to its information assets, and which enables the continued sound operations of the banking corporation.

14. The board of directors shall outline the IT strategy including the risk appetite, and devote an in-depth discussion to the IS and the cyber defense strategy included in it. The goal of the strategy is, among other things, to protect the banking corporation against existing and emerging IT risks, including IS-related risks, all in accordance with Proper Conduct of Banking Business Directive No. 301 on "The Board of Directors" (hereinafter, "Directive 301"), Directive no. 310, and Directive no. 350. The IT strategy shall be consistent with the banking corporation's overall business strategy and define a comprehensive outline that guides IT management and IS and cyber defense management in the banking corporation. The outline shall include overarching objectives and programs for all areas of IT that affect the banking corporation, including cost management, human resources management, software and hardware management, third party management, risk management, identification of the banking corporation's relevant reference threats, and all other considerations of the organization's IT array.

    The strategy shall, among other things, refer to the manner in which the IT should evolve to support and participate in implementing the banking corporation's business strategy, including in response to the evolution of the organizational structure, changes in the IT, and key areas in which relationships with third parties are maintained. The strategy should be updated as necessary, and in any case at least once every three years.

15. The board of directors shall discuss, decide, and approve the IT management policy and the IT risk management framework, which are a function of the strategy determined by the board, and shall ensure that the banking corporation's senior management takes the necessary steps to implement them, all in accordance with this Directive and with Directives 301, 310, and 350. In said discussions, the board of directors shall devote an in-depth discussion to the IS and cyber defense management framework, including the IS and cyber defense management policy.

16. The board of directors should ensure that:

    16.1. the scope and skills of the human resources in all three lines of defense in the banking corporation are sufficient to continuously support the needs of the IT array and the IT risk management processes, and to implement the banking corporation's IT strategy;

    16.2. the budget allocated to the achievement of these goals for all three lines of defense is sufficient.

17. To carry out its duties pursuant to Sections 13–15 above, the board of directors should understand the banking corporation's IT operations and the risks they entail, and establish processes to monitor and assess the effective implementation of the banking corporation's IT strategy. The board of directors should perform the following actions, among others:

    17.1. promote effective IT corporate governance, including aspects related to IT risk management;

    17.2. define, for management, the manner in which the board wishes to be involved in various IT issues, including the banking corporation's IT risks and the principles of authority delegation, risk escalation, and required reporting, including the scope, contents, and frequency of the reports;

    17.3. ensure that the banking corporation's IS capability and the investment therein are appropriate, in view of the IS risks that the banking corporation faces and with respect to the execution of the defined strategy;

    17.4. ensure the existence of processes designed to ensure the banking corporation's compliance with the legal and regulatory requirements related to IT, IS, and cyber defense, and with the determined IT risk management framework, based on, among other factors, tests conducted by the compliance function and reviews performed by senior management, including the Chief Risk Management Officer and the Internal Auditor;

    17.5. conduct a discussion at least annually, and as necessary, to challenge management regarding the effectiveness of the IT management policy and the effectiveness of the IT risk management framework, including the effectiveness of the control environment and the integrity of the information assets. To this end, the board of directors shall, inter alia, review the adequacy of the test coverage (see Chapter I hereinafter "Assessing the Effectiveness of Information Security Controls") performed on the control environment, material deviations from the framework and how they are handled, an analysis of incidents in which IT risks materialized, including IS incidents, and a comparison with accepted practices. Upon the occurrence of an incident requiring senior management to report immediately to the board of directors, a discussion on the matter shall be held as soon as possible (see Section 19.9 hereinafter);

    17.6. ensure that the internal audit work plan, developed in accordance with Proper Conduct of Banking Business Directive No. 307 on "The Internal Audit Function" (hereinafter, "Directive 307") and this Directive, also includes appropriate work plans for inspecting the adequacy of the IT array and the IT risk management framework,

and that the internal audit function has the proper skills, capacity, and capabilities to provide an independent opinion on said appropriateness;

17.7. The board of directors should develop its position on the effectiveness of the controls, based on the findings of the internal audit, and if necessary should consider using additional expert opinions or other means;

17.8. annually discuss, decide, and approve the annual and multi-annual IT work plans, including the work plan for addressing IT risks;

17.9. hold a meeting with the Chief Technology Officer and a meeting with the Chief Cyber Defense and Information Security Officer (CISO) at least once a year, in order to assist the board in assessing the effectiveness of the IT management framework and the IT risk management framework in the banking corporation.

18. In all the discussions conducted pursuant to Section 17 above, the board of directors should also address issues arising from the banking corporation's use of third parties to manage its information assets.

**Senior management**

19. The banking corporation's senior management is responsible for the implementation and maintenance of an appropriate, secured operations environment that supports the banking corporation's objectives and its goals and complies with the relevant statutes and regulations. Within this responsibility, senior management is responsible for IT performance and its ongoing operations. To this end, the banking corporation's management should:

19.1. implement effective IT governance, including allocation of areas of responsibility and authority according to the principles to be outlined by the board of directors, and regulation of the manner of supervision and coordination between the CTO and the CISO and the various entities that comprise this field, and their interfaces shared with the various entities and with external parties;

19.2. plan and implement the IT risk management framework;

19.3. develop an IT management policy and IT risk management policy;

19.4. develop annual and multi-annual work plans in the field of IT and for managing the risks the plans entail, and allocate proper resources for its implementation;

19.5. maintain and update IS capability to ensure the banking corporation's continued proper operations;

19.6. determine priorities and coordinate between the function in charge of IT and the business lines;

19.7. outline and monitor the coordination of IS activities with internal risk management functions (see Section 30 hereinafter) and with external functions (see Section 28.14 herein, and ensure that a process exists for receiving, analyzing, and responding to intelligence on threats and vulnerabilities, for example participating in collaborative programs on this issue;

19.8. receive and provide periodic reports to the board of directors on the following issues:

19.8.1. IT risks and how they are handled;

19.8.2. relevant (internal and external) IS incidents and analyses of their implications;

19.8.3. execution of the IT strategy;

19.8.4. material changes in the field of IT;

19.9. provide immediate reports to the board of directors regarding any material deviation from the IT management policy or the IT risk management framework (see Section 22 hereinafter), material adverse development in IT risks, a material change in the information assets or the business environment, and technological failure incidents and IS incidents that potentially have a significant impact on the banking corporation;

19.10. implement processes that ensure compliance with the legal and regulatory requirements in the field of IT, including compliance with the IS management framework;

19.11. establish a process to map the information assets and implement risk-mitigating measures as detailed in Chapter C: "The IT Risk Management Framework (General)";

19.12. ensure that the appropriate hiring and employee training procedures and processes are in place to maintain their competence and suitability for their roles, as detailed in Chapter D: "The Human Factor – User Training and Awareness":

19.13. regulate an IS control effectiveness assessment process as detailed in Chapter I "Assessing the Effectiveness of IS Controls";

19.14. establish principles for incident and problem management as detailed in Chapter K "Incident and Problem Management";

20. Senior management should ensure the effectiveness of the IT management policy and the IT risk management framework over time, including:

20.1. Senior management of the banking corporation should conduct the following periodic discussions to ensure that the steps taken to implement the IT strategy, including the IT risk management strategy, remain relevant and appropriate:

20.1.1. an annual discussion on the IT management policy and work plan, IS capability, and the IS and cyber defense policy and work plan;

20.1.2. periodic discussions on the achievement of the work plan objectives;

20.1.3. at least one discussion each year on the information asset mapping process and implementation of technological controls, including IS controls;

20.1.4. additional discussions in the following events: material findings emerge from the process of monitoring the IS management framework, material changes were made to the IT risk management framework, and other material issues such as significant commitments.

20.2. Senior management should revise the IT management policy and the IT risk management framework as necessary, including the procedures, controls, and risk

assessment process, and allocate the necessary resources to execute its decisions while maintaining IS capability pursuant to the board of directors' resolutions.

21. Senior management of the banking corporation shall appoint a CTO and a CISO, as detailed in Sections 23 and 28 hereinafter, and must ensure they have the required resources to perform their duties.

22. Pursuant to the policy to be defined, the banking corporation's senior management shall establish procedures for special situations in which a deviation from the IT management policy or the IT risk management framework is expected to occur or has occurred. Such procedures shall, inter alia, address the following aspects: documentation of deviations, authorizations for approving deviations, validity of the deviation approvals, and oversight of approved deviations. When a deviation is approved, the banking corporation shall ensure that compensating controls are in place.

**The Chief Technology Officer (CTO)**

23. A banking corporation shall appoint a manager who is a member of management and bears explicit responsibility for the totality of IT-related issues (hereinafter, "CTO"). The CTO must have the appropriate professional qualifications and proven experience in the field of IT and IT management.

24. Within the CTO's responsibility for all IT-related issues, the CTO is responsible for the IT, including its ongoing operations and management, its IS, and operational resilience, including among other things:

    24.1. development and implementation of the IT strategy, taking into account the instructions of the board of directors and senior management;

    24.2. development and implementation of the IT management policy (see Section 54 hereinafter), taking into account the instructions of the board of directors and senior management;

    24.3. development and implementation of the annual and multi-annual IT work plan. On this issue, also see Section 64 "IT planning and investment process," hereinafter.

    24.4. management of the IT budget;

    24.5. management of the performance of resources in the field of IT;

    24.6. capacity management – See Section 61.6 hereinafter;

    24.7. management of IT-related procurement and investments;

    24.8. appropriate professional development and training;

    24.9. implementation of the IT architecture – See Section 57 hereinafter;

    24.10. support of the business lines' operations, including the aspects of these operations related to IS, operational resilience, and reporting on IT risks, all while adapting the IT to the business requirements;

    24.11. the existence of appropriate processes and controls to ensure that all IT risks are identified, analyzed, measured, monitored, controlled, reported, and contained within the limits of the banking corporation's risk appetite, and to ensure that the projects

and systems that it provides and the activities that it performs comply with the requirements of internal and external parties;

24.12. integration and control of technological failure incidents in the banking corporation.

25. CTOs shall have no additional responsibility that might interfere with their functioning.

26. The banking corporation must notify the Supervisor of Banks 30 days in advance of the anticipated departure of the CTO, and upon the appointment of an acting CTO for a period exceeding one month — 30 days before the commencement of their service, or upon a decision to appoint them, the later of the two dates.

**Lines of business managers**

27. In addition to the CTO and the CISO, the lines of business managers also have IT responsibilities. The division of responsibility between the lines of business' managers and the CTO and CISO will be determined according to the banking corporation's policy and the processes that are established. The following are examples of issues in which responsibilities are divided:

27.1. establishing processes for informing the IT function of business needs, required reports from the information systems, and plans for launching new products;

27.2. ensuring that IT development plans are prioritized, budgeted, and aligned with the business lines' business strategy;

27.3. ensuring that required backup of the technological systems and processes that support the business line's operations are available;

27.4. retaining documentation of the business line's processes, and informing the CISO of any change in these processes;

27.5. performing due diligence reviews for prospective third party providers and monitoring the activities of existing third party providers;

27.6. discussing the IS risks inherent in the business line's new business initiatives, with the CISO.

**Chief Cyber Defense and Information Security Officer (CISO)**

28. A banking corporation shall appoint a senior employee as the CISO, who will be subordinate to a member of the banking corporation's management and responsible for monitoring and ensuring that the banking corporation complies with the IS management framework, and within this responsibility will be responsible for oversight and reporting regarding IS risk management and mitigation, and the CISO's area of operations will encompass all the banking corporation's business lines and corporate-wide strategic business aspects. The CISO's duties include:

28.1. integration of issues related to IS and cyber defense management in the banking corporation;

28.2. consulting to senior management on IS and cyber defense management;

28.3. assistance to management in developing and implementing an IS and cyber defense policy (see Section 106 hereinafter);

28.4. development of a corporate IS risk management methodology;

28.5. development, follow-up on implementation, and monitoring a detailed and comprehensive plan on how the banking corporation addresses IS risks, as stated in this Directive;

28.6. establishment of principles and work processes for implementing IS and cyber defense controls;

28.7. initiation, promotion, and implementation of processes designed to increase users' awareness of IS and cyber defense, including appropriate training programs on IS risks for the board of directors, senior management, employees, third parties, and customers (see Chapter D "The Human Factor – User Training and Awareness");

28.8. establishment of a reporting framework for the reports from various functions in the banking corporation;

28.9. initiation of tests to assess the effectiveness of IS controls, as stated in Chapter I "Assessing the Effectiveness of IS Controls."

28.10. performing due diligence of third parties with respect to IS and cyber defense aspects, and monitoring the activities of existing third parties in these areas;

28.11. keeping apprised of the IS risks in new business ventures and establishing methods to mitigate these risks through dialogues with business line managements and other means;

28.12. keeping apprised of information flow processes and the risks to the information in these processes, and the IS and cyber defense measures required, through dialogues with business line managements and other means;

28.13. development of relevant metrics, preparation of reports, and reporting, as required according to Directive No. 350;

28.14. coordination and communications on IS and cyber defense issues, including sharing information and intelligence with external entities for defense purposes as permitted by law. Examples of external entities are regulatory entities, investigative and enforcement entities, the National Cyber Directorate, the Cyber and Finance Continuity Center at the Ministry of Finance, corresponding IS risk management functions in the financial sector, and third parties' risk management functions;

28.15. integration and control of IS incident management in the banking corporation, including reporting on material IS incidents to the board of directors, management, and relevant authorities, as stated in Chapter K "Incident and Problem Management."

28.16. initiation and execution of exercises, as stated in Chapter K "Incident and Problem Management."

28.17. leading and coordinating processes related to IS and cyber defense management;

28.18. analysis of significant IS incidents in Israel and worldwide, learning lessons from those incidents, and implementing the relevant conclusions in the banking corporation.

29. The CISO will be granted appropriate status and authority.

30. The CISO will ensure the establishment of interfaces with the various functions that make up the IS risk management framework such as technology units, business units, Chief Risk Officer, compliance function, Director of Business Continuity, legal counsel, training, HR, and security. The CISO will be responsible for coordinating and integrating all the entities that comprise the framework.

31. CISOs will have the appropriate qualifications, relevant professional training, and adequate experience for performing their duties.

32. CISOs will ensure that they continuously keep abreast of new IS management methodologies and technologies, which includes communications with professional entities in this field, both within and outside the banking system.

33. CISOs will not bear any additional responsibility that might interfere with their functioning, and their duties and responsibilities will not create a conflict of interest for them, specifically with respect to their executive duties in the field of IT.

34. The banking corporation must notify the Supervisor of Banks 30 days in advance of the appointment and anticipated departure of the CISO, and upon the appointment of an acting CISO for a period exceeding one month—30 days before the commencement of their service, or upon a decision to appoint them, the later of the two dates.

**Risk management function**

35. The risk management function will:

    35.1. oversee and ensure that IT risks are properly managed pursuant to the principles outlined in Directive 310 and Directive 350.

    35.2. without prejudice to the provisions of Section 11(b) of Directive 310, the risk management function will be independent of the first and third lines of defense and will operate independently from the IT system's operational processes.

    35.3. without prejudice to the provisions of Section 11(a) of Directive 310, the risk management function's responsibilities include but are not limited to:

        35.3.1. assisting the CEO in developing and maintaining policy, procedures, and instructions, with the involvement of all the relevant entities;

        35.3.2. developing and maintaining the IT risk assessment and management methodology;

        35.3.3. monitoring and controlling the banking corporation's compliance with the IT risk management framework. The risk management function will ensure that IT risks are identified, measured, assessed, controlled, monitored, and reported.

    A key duty of the IT risk management function is to challenge the adequacy of the business lines' inputs into the banking corporation's IT risk management, risk assessment, and reporting systems, and the adequacy of the outputs.

**Internal audit**

36. A banking corporation shall include within its internal audit function, an organizational unit for the purpose of IT auditing. The person in charge of internal IT auditing must have the relevant professional training and experience for performing audits in this field.

37. Development of the internal audit work plan required according to Directive no. 307 will consider the totality of the IT operations, corporate governance, and IT functions and processes including those in the field of IS. The internal audit plan will include an examination of the design and effectiveness of the technological controls, including IS controls, and controls implemented by third parties over the banking corporation's information assets, such that all the aspects of the IT control environment are examined periodically. The frequency of the examination and its scope will be a function of the potential impact of deficiencies in technological controls, including IS controls, based on the judgment of the internal auditing function; the internal auditing function's ability to rely on other tests conducted on those controls; and changes in vulnerabilities and threats or material changes in the information assets.

38. In each of the following events, the internal audit function will assess the scope and quality of the work performed in order to determine its degree of reliance thereupon:

    38.1. reliance on work performed by other entities in the banking corporation;

    38.2. use of outsourcing to perform internal audit activities, as described in Directive 307;

    38.3. reliance on tests performed by a third party for activities it performs on behalf of the banking corporation .

39. For the purpose of conducting real-time audits in the field of IT, IS, and cyber defense, the internal audit must define a methodology that includes, but is not limited to, reference to the following issues:

    39.1. defining strategic technological projects that require a real-time audit task and defining its involvement in the various stages of the lifecycle of the information asset to which the project refers;

    39.2. defining its real time involvement in the incident and problem management process determined by the banking corporation. See Chapter K "Incident and Problem Management."

## Chapter C: IT Risk Management Framework (General)

**Organization and objectives**

40. A banking corporation must establish an IT risk management framework, and for this purpose will define and assign key duties and areas of responsibility and appropriate reporting lines to ensure that the framework is effective. The IT risk management framework will be fully integrated into and aligned with the banking corporation's overall risk management processes.

41. A banking corporation's IT risk management shall comprise the three lines of defense required by Directive 310, while incorporating and implementing the following documents

and processes, among others:

41.1. its IT strategy, including its risk appetite for IT risks;

41.2. its IT risk management policy stemming from the strategy;

41.3. identification and assessment of the IT risks to which the banking corporation is exposed;

41.4. definition of the risk-mitigating measures, including controls;

41.5. monitoring the effectiveness of the risk-mitigating measures and monitoring technological failure incidents and IS incidents (see Chapter K "Incident and Problem Management"), and taking steps to correct them, including implementation of appropriate controls, as necessary;

41.6. reporting to senior management and the board of directors regarding the IT risks and the implemented controls;

41.7. identification and assessment of the IT risks that result from material modifications to IT, its processes, and its procedures, or from significant technological failures incidents or significant IS incidents.

The areas of responsibility and activity for each line of defense will be in accordance with the provisions of Directives 310 and 350.

42. A banking corporation shall ensure that its IT risk management framework is continuously documented and updated according to the lessons learned during its implementation and monitoring.

**Identification and classification of activities, processes, and information assets**

43. Activities, processes, and information assets must be identified and classified as follows:

43.1. Financial institutions must identify, establish and maintain updated mapping of their business activities, roles and supporting processes to identify the importance of each and their interdependencies related to IT risks.

43.2. Based on the mapping process described in Section 43.1 above, a banking corporation shall identify, establish and maintain updated mapping of all its information assets including those managed by third parties. The mapping process will also include identification and documentation of the interrelations among the information assets, in order to, among other things, facilitate responses to technological failures incidents and IS incidents.

43.3. A banking corporation shall classify its business activities, supporting processes, and information assets in terms of criticality and sensitivity. This classification will reflect the potential financial or other impact caused to the banking corporation or its stakeholders by the occurrence of a technological failure incident or IS incident that affects business activities, supporting processes, or information assets.

43.4. A banking corporation shall implement a process that identifies where the classification of information assets, business activities, and supporting processes requires change as well as allowing for the classification of new information assets,

business activities, and supporting processes. This process must be undertaken at least annually, or when there is a material change to the regulated entity's information assets, business activities, and supporting processes or business environment.

**Methodology for identifying and classifying business activities, supporting processes, and information assets**

44. A banking corporation must establish and document an identification and classification methodology that defines principles that include but are not limited to defining what constitutes an information asset, business activity, and supporting process; the required mapping granularity; and principles for rating criticality and sensitivity.

    44.1. The required level of granularity will be of such that allows rapid identification of an information asset, its location, and the asset's owner, within the meaning of this term in Section 45 hereinafter, and will be sufficient to determine the nature and strength of controls required to protect the information assets, business activities, and supporting processes.

    44.2. Where a banking corporation has chosen to aggregate a number of underlying components into a single information asset or a single business activity, or a single supporting process, the criticality and sensitivity rating for that information asset, business activity, or supporting process would inherit the criticality and sensitivity ratings of the constituent components with the highest ratings.

45. An information asset owner shall be defined for each information asset and the information asset owner will be in charge of managing the information asset and providing reports with respect to it.

**Risk assessment**

46. A banking corporation must carry out a risk assessment on an ongoing basis, in which it identifies and assesses the IT risks that affect its business activities, supporting processes, and identified information assets, based on their criticality and sensitivity. The risk assessment must be documented and updated, specifically when a material change occurs in infrastructures, processes, or procedures that affect the banking corporation's business activities, supporting processes, or information assets.

**Risk mitigation**

47. A banking corporation must define and implement the required measures, including appropriate controls or modifications to its processes, in order to mitigate the IT risks identified pursuant to Section 46 above, and ensure that they are aligned with its risk appetite; These measures include determining whether changes are needed in its existing business processes, controls, or IT array.

48. The controls to protect information assets must be defined and implemented according to, among other things, the criticality and sensitivity ratings assigned to them, and to the principles detailed in Chapter H "Implementation of IS Controls."

**Reporting**

49. A banking corporation shall report the results of the risk assessments to senior management in a clear and timely manner.

## Chapter D: The Human Factor - User Training and Awareness

50. In this Chapter, the term "employees" includes contractors who are managed by the banking corporation.

51. A banking corporation shall develop and conduct training programs for existing employees on new technologies and products before their launch, and develop training programs for new employees who will be on-boarded as necessary. In addition, the banking corporation must ensure that periodic training sessions to refresh employees' knowledge are conducted as necessary.

52. A banking corporation shall ensure continuity in key roles within the IT array, including IS, through appropriate agreements, professional development programs, training and instruction programs of alternative employees as necessary, and backup plans for filling these positions on a provisional basis.

53. A banking corporation shall establish a training and awareness program on topics related to IS and cyber defense and to privacy protection, to be conducted for all employees periodically, and at least once a year. The program will train employees to perform their duties in a manner that is aligned with the banking corporation's IS policy and procedures and will train employees how to deal with IS-related risks.

    The banking corporation shall ensure that third parties' employees who are not managed by the banking corporation also undergo a training and awareness program on IS, cyber defense, and on topics related to privacy protection, as stated above, according to the criticality and sensitivity of the information asset to which they have access.

# Part C – Information Technology Risk Management

## Chapter E – IT Management

**IT management policy**

54. The IT management policy must be documented and must address the manner of IT management, including IT operations, monitoring, and controls, and detail the enterprise-level processes related to technology design and planning in order to meet the banking corporation's business needs (see additional information in Section 57 on "Architecture" hereinafter), to implement appropriate technological infrastructures (see additional information in Section 58 on "Technological Infrastructure" hereinafter), and to deliver financial services and products to its customers (see additional information in Sections 59–63 on "Operations " hereinafter). The policy will emphasize, among other things, aspects pertaining to technology risk management, the adequacy of IT information security, customer protection, and compliance with applicable laws and regulations

55. A banking corporation shall ensure that its information systems allows the board of directors

and management to assess the banking corporation's business performance, identify the risks and challenges that it faces, and assist in its operations. To this end, the banking corporation's information systems must meet the following characteristics while implementing appropriate controls:

55.1. provide accurate, consistent, complete, relevant and timely information;

55.2. be reliable so that they can be relied upon for the purpose of documentation and information collection;

55.3. provide key risk performance trends and indicators;

55.4. support the banking corporation's business strategy;

55.5. ensure data confidentiality, integrity, and availability;

55.6. Reduce labor-intensive manual activities as far as possible;

56. When determining a policy as stated in Section 54 above, the banking corporation must ensure that issues related to operational resilience are integrated in planning, implementation, and operational processes as follows:

56.1. The banking corporation must ensure that IT planning, implementation, and operational processes provide operational resilience that allows it to continue to provide essential activities to its customers even during a disruption. To this end, the banking corporation must ensure that it actively integrates into said processes measures to protect IT confidentiality, integrity, and availability and to reduce the risk of such events, and integrates said processes into the project management process and the business continuity plan.

56.2. When using a cloud computing environment to provide essential activities to customers or when planning a transition to such an environment, the banking corporation must verify the operational resilience of said environment and include this requirement in its contract with the third party that provides the cloud computing services.

**Architecture**

57. A banking corporation must implement principles for planning and designing effective IT architecture, including:

57.1. The banking corporation must plan, implement, and adjust its IT architecture to the strategic and business objectives that it defined for itself, and must develop an appropriate plan for this purpose that meets the requirement to maintain IT confidentiality, integrity, and availability in order to minimize operational and reputational risks arising from improperly designed systems.

57.2. The architecture plan will detail the overall IT array design and the principles that describe the banking corporation's operating framework, including its tasks, businesses and customers, the flowcharts of its operations and processes, data processing processes, interfaces with IT, IS, and availability. The degree of detail will be determined according to the criticality and sensitivity of the information assets.

57.3. The architecture plan must be developed so that it assists the banking corporation in, but not limited to, the following tasks:

57.3.1. Designing the IT array concept and ongoing maintenance of the IT array structure, controls, policy, and related policy and procedures;

57.3.2. Maintaining an up-to-date list of the information assets, the business activities, and the supporting processes. See Section 43 above.

**Technological infrastructure**

58. A banking corporation shall apply principles for establishing of an adequate technological infrastructure, including the following:

58.1. In implementing technological infrastructure, whether managed by the banking corporation or by a third party, the banking corporation must ensure that the infrastructure maintains and promotes aspects of confidentiality, integrity, and availability, as well as the banking corporation's business objectives. To this end, the banking corporation must develop, document, and implement—according to the criticality and sensitivity of the information assets—appropriate policies and procedures for assimilating infrastructure controls that protect the facilities, technology, and data. These controls shall include aspects of redundancy and resilience for technological infrastructure components, as well as for related products, services, and communications. The policy and the procedures must cover the following issues, among others:

58.1.1. processes for identifying, tracking, and monitoring technological infrastructure components;

58.1.2. appropriate allocation of resources, including appropriate knowledge and expertise, to the field of technological infrastructure;

58.1.3. network configuration management and change management processes. See Chapter F hereinafter on "Project Management and Change Management."

58.1.4. security and monitoring processes for analyzing data traffic and detect anomalous activities;

58.1.5. system development processes that address scalability, interoperability, portability, adequate software controls, and use of and controls over open source software;

58.1.6. mainframe controls, to address unique risks associated with mainframes;

58.1.7. physical access controls and environmental controls. See Section 122 hereinafter "Physical access and environmental controls."

58.2. The banking corporation's technological infrastructure must support the banking corporation's operational resilience in accordance with the criticality of the information asset to the corporation’s essential processes and services.

**Operations**

59. A banking corporation must apply the following operations principles, including:

    59.1. A banking corporation must establish an IT operations framework that supports the activities and services that IT provides, manages information assets, manages changes, provides appropriate responses to incidents, and ensures the stability of the production environment;

    59.2. A banking corporation must periodically ensure that the IT operations meets the requirements and business objectives that it determined for itself;

    59.3. A banking corporation must ensure the integration into its IT operations aspects of operational resilience that will assist in preventing losses, protect sensitive customers information, and minimize disruptions to service delivery;

    59.4. A banking corporation must ensure that it maintains the efficiency of the activities and services that the IT system provides and improves it as much as possible;

    59.5. The operations framework will include but is not limited to the development and implementation of the controls and processes described in Sections 60–63 hereinafter.

***Operational controls***

60. A banking corporation must develop and implement operational controls to safeguard its overall operational environment, including its physical facilities; infrastructure supporting operations, systems, software; and controls addressing human factors. Examples of such controls include physical and logical access controls over the banking corporation's operating centers, identity management controls, careful selection processes that ensure an employee's suitability for a job, appropriate segregation of duties, and implementation of dual control to prevent any one person from performing a complete process (see additional information on some of these controls in Chapter H "Implementation of IS Controls").

***IT operational processes***

61. A banking corporation must develop IT operational processes to reduce potential operational failures including those stemming from manual actions, and minimize the impact of issues that occur. These processes include but are not limited to:

    61.1. **Maintenance** – A banking corporation must implement, according to the criticality and sensitivity of the information asset, a process to prevent malfunctions of information assets, or a process that restores operational capabilities to their original state following the occurrence of such a malfunction;

    61.2. **Configuration management** – A banking corporation must implement a process to maintain essential information concerning the software and hardware configuration components of an information asset (e.g., model, version, specifications) according to its criticality and sensitivity, and review and confirm the information in an ongoing manner to ensure that it is accurate and up to date;

    61.3. **End of Life/End of Support -** A banking corporation must implement a process to identify software or hardware with limited support, support that is expected to be

discontinued, or no support, whether provided by a third party or in-house. This process includes a risk assessment of the potential risks, including IS risks, that may stem from the future use of such identified software or hardware, and must implement appropriate controls to minimize these risks, for example, by separating the information asset from other information assets. If necessary, the banking corporation must decommission the software or the hardware;

61.4. **Patch management** – A banking corporation must establish a process that ensures the implementation of functional and nonfunctional patches (e.g., fixes for security vulnerabilities or software bugs) within a timeframe that is commensurate with the criticality and sensitivity of the patch and the information asset. Patches must be tested in a separate environment before applying them in the production environment to ensure compatibility with the existing information assets and that they do not cause IT failures;

In the matter of emergency patches to which the ordinary patch management process cannot be applied, see Section 97 hereinafter.

61.5. **Backup management** -

61.5.1. A banking corporation must establish a backup and recovery process for information assets to ensure their recovery when necessary. The scope and frequency of the backups must be adjusted to the business recovery requirements and the criticality and sensitivity of the information asset, and must be revised according to changes in the risk assessment. The banking corporation must ensure that the backups are stored in a secured manner and at a sufficient distance from the main site so that they are not subject to the same risks as the main site. Testing of the backup and recovery process must be undertaken on a periodic basis.

61.5.2. The information asset backup and recovery process must also be designed to be appropriate for scenarios in which attempts are made to undermine the credibility of the backups, and include retrieval and recovery from backups even in the event of harm to the backup process itself.

61.5.3. A banking corporation that uses a third party to manage its backup process must ensure that the third party performs the aforesaid process.

61.6. **Capacity and performance management** -

61.6.1. A banking corporation must establish capacity management processes that take into account anticipated internal factors, such as an increase in the scope of the banking corporation's business, mergers, acquisitions, new products, and implementation of new technologies, and anticipated external factors such as shift in customer demands and market requirements.

61.6.2. A banking corporation must assess its IT array capacity in an ongoing manner in order to ensure appropriate performance, with respect but not limited to the platform processing speed, primary working memory for each platform’s central processing unit (CPU), additional data storage

capacity, and data transfer bandwidth.

61.6.3. A banking corporation must analyze capacity trends in order to ensure that it continues to meet its business requirements.

61.6.4. A banking corporation must periodically analyze projected capacity needs compared to actual capacity in order to determine whether the capacity planning and management processes are appropriate and to revise them as necessary.

61.6.5. Upon developing or acquiring new technologies, the banking corporation must take into consideration, among other things, the flexibility of the systems based on these technologies with reference to the expected capacity requirements.

61.6.6. Upon entering into an agreement with a third party, a banking corporation must assess the third party's performance and its own performance in order to determine whether the capacity adequately meets current and future business requirements.

61.7. **Management of log-based audit trails** -

61.7.1. A banking corporation must establish a process for generating, transmitting, storing, analyzing, and disposing of log-file-based audit trails that will be used in the identification, tracking, analysing, and resolution of various IT incidents, including IS incidents. An audit trail will contain information on access, actions, and queries of users in the banking corporation's information systems. The information to be stored must include the identity of the accessing entity, the source, the timestamp, and details about the access target.

61.7.2. Notwithstanding the provisions of Section 61.7.1 above, with respect to queries of the banking corporation's employees, the banking corporation shall keep an audit trail at its discretion, on the basis of the risk assessment.

61.7.3. Access to the audit trail must be secured in order to prevent unauthorized modification or deletion or abuse of the data collected in the audit trail, and the audit trail must be retained for an appropriate period, according to the criticality and sensitivity of the business activities, the supporting processes, and the information assets, and according to the legal and regulatory requirements that apply to the banking corporation.

61.7.4. A banking corporation must employ tools, according to an appropriate risk assessment, for automated analysis of the audit trail, which will help to identify anomalies, important events, and patterns of activity, among other things.

61.7.5. Upon entering into an agreement with a third party, the banking corporation must review, according to the risk assessment among other things, the need to include in the contract with the third party a requirement to transit log files from its systems, at the banking corporation's request.

61.8. **Disposal of data and media -**

61.8.1. A banking corporation must establish a process for deleting data and disposal or transferring physical media (e.g., print-outs) and digital media (e.g., hard drives, storage devices), commensurate with the criticality and sensitivity of the information asset and type of media used. The method of deletion or disposal must be determined according to the type of data to be deleted. The banking corporation must consider deleting data on media whenever media are transferred between departments.

61.8.2. A banking corporation must establish a process for transferring or disposal of equipment (e.g., printers) that may contain residual data. The process must also refer to the need for a periodic review of the IT environment to ensure the timely disposal of decommissioned equipment.

61.8.3. A banking corporation that enters into an agreement with a third party must include in the contract arrangements for deleting, after the termination of the agreement or at the banking corporation's demand, the banking corporation's data stored by the third party or stored by parties that have entered into agreements with said third party for the purpose of executing the agreement between the banking corporation and the third party. The data deletion arrangement must be aligned with the banking corporation's disposal of data process. See Section 61.8.1 above.

In the event of any inconsistency between this requirement and the requirement that appears in Section 30(a) of Proper Conduct of Banking Business Directive No. 362 "Cloud Computing" (hereinafter, "Directive 362"), the more stringent requirement shall apply.

***Service and Support Processes***

62. A banking corporation must develop and implement IT service and support processes that ensure the achievement of its strategic goals and objectives that it defined for itself, by ensuring continuous reliability and resilience of IT; support of the business lines, employees, and customers; and prevention of IT malfunctions. These processes must also include the "Incident and Problem Management" processes – Chapter K hereinafter.

***Monitoring, Evaluating, and Reporting Processes***

63. A banking corporation must develop processes:

63.1. for ongoing monitoring of IT operations. See Chapter J "Monitoring IT."

63.2. for periodically evaluating and reporting the effectiveness of the implemented controls to senior management. Evaluating the effectiveness of the controls will assist senior management in identifying emerging trends in the risks entailed in IT operations, such as ineffective controls, inefficient processes, insufficient or inefficient use of resources, and substandard service delivery.

The banking corporation must establish a process for periodically reviewing the monitoring, evaluating, and reporting processes and adjust them to emerging requirements and objectives.

**IT planning and investment process**

64. A banking corporation must apply principles for the proper implementation of an IT planning and investment process:

    64.1. A banking corporation must implement an appropriate IT planning and investment process that includes preparedness for future activities by defining objectives and strategies for achieving them. The board of directors, senior management, and the employees must participate in the process. The process must be integrated in the overall business planning process and be continuously adjusted to new risks and business opportunities. The products of the process will be strategy documents, policies, and work plans. The process must address, but is not limited to, the following issues:

        64.1.1. the banking corporation's short-term and long-term objectives and the resources allocated to achieve them;

        64.1.2. alignment of the IT strategy with the banking corporation's business strategy;

        64.1.3. Identification and measurement of risk before changes or new investment in technology are made;

        64.1.4. existence of the appropriate technological resources (e.g., infrastructure, operating software, applications, and employees) to support the current and anticipated business operations.

    64.2. As part of the planning process, a banking corporation that enters into an agreement with third parties must ensure that the third party's plans and actions support the banking corporation's plans and do not adversely affect them.

## Chapter F: Project Management and Change Management

**IT project management**

65. A banking corporation must implement an IT project management framework that ensures consistent use of accepted practices in this field and also ensures that project outcomes meet their defined requirements and objectives. At a minimum, the framework shall define roles and responsibilities, accountabilities, and reporting lines, to effectively support the implementation of the IT strategy. The framework should distinguishing between types of projects according to the criticality and sensitivity of the information asset relevant to each project, and in accordance with project characteristics relevant to the banking corporation, such as size and complexity, significance for implementing the banking corporation's strategy, and innovativeness.

66. A banking corporation must implement a process to properly identify and assess the risks stemming from its IT project portfolio and to take steps to mitigate these risks. Within these efforts, the banking corporation must also address risks that may stem from interdependencies between different projects and from dependencies of multiple projects on the same resources or expertise.

67. A banking corporation must establish an IT project management policy that includes, but is not limited to reference to the manner of implementation of the following issues across project types:

    67.1. project objectives;

    67.2. roles and responsibilities, including project approval authorization;

    67.3. project risk assessment and risk mitigating measures;

    67.4. project plans, timeframe and steps;

    67.5. key milestones;

    67.6. change management requirements.

68. The IT project management policy must ensure that IS requirements are analyzed and approved by a function that is independent from the development function and which was approved by the CISO.

69. A banking corporation must ensure that, for the purpose of executing an IT project, representatives from all the areas affected by the project are assigned to the project team, and the team has the required knowledge to ensure appropriate project implementation.

70. A banking corporation must report to the board of directors, according to the policy to be defined, on the execution of IT projects and progress in their completion, including their associated risks, either individually or in aggregation, depending on the significance and scope of each project, both in an ongoing manner and on an ad hoc basis as appropriate.

71. A banking corporation must include reference to project risk in its risk management framework.

**Systems acquisition, development, and implementation**

***General***

72. A banking corporation must establish a risk-based process to manage systems acquisition and development, and implementation of acquired systems.

73. Prior to each system acquisition or development, a banking corporation must ensure that the functional and non-functional requirements, including IS requirements, are clearly defined and approved by the management of the relevant business function.

74. A banking corporation must implement a methodology to test and approve the system prior to its initial use. This methodology must take into account the criticality and sensitivity of the information asset, among other factors. The test must ensure that the new system functions properly, and the test must be conducted in a test environment that simulates the production environment as far as possible.

***System Acquisition***

75. The system acquisition management process must refer, but is not limited to, an evaluation and selection of the third party to ensure that it has the appropriate capabilities to comply with the requirements and deliver the system. The level of the evaluation and due diligence carried out must be commensurate with the criticality and sensitivity of the information asset.

76. According to an appropriate risk assessment, a banking corporation must evaluate the robustness of the third party's software development and its QA practices, and ensure the implementation of control measures, including appropriate IS controls over any sensitive information to which the third party has access to over the course of the project. Any access by a third party to information assets within the project must be monitored and controlled, among other things, pursuant to the provisions of Section 61.7 above "Management of log-based audit trails."

77. If the project uses off-the-shelf or open source solutions that do not comply with the requirements of the banking corporation's IS management framework, the banking corporation must assess the risks and ensure the existence of compensating controls before the project is deployed.

78. A banking corporation must evaluate the necessity of a source code escrow agreement, according to the criticality and sensitivity of the information asset, and must define alternatives in the event that an escrow agreement is necessary but cannot be implemented.

***System Development and Implementation***

79. A banking corporation must ensure that measures were taken to mitigate the risk of unintentional modifications or intentional manipulations of the system during the development process or implementation in the production environment.

80. A banking corporation must comprehensively document the development, implementation, operations, or configuration of the systems in order to minimize any unnecessary dependency on outside experts. At minimum and to the extent feasible, the documentation must include user documentation, technical system documentation, and operating procedures.

81. A banking corporation must implement a physical or logical separation between the production environment and the development, testing, and other non-production environments, in order to ensure adequate segregation of duties and to prevent the introduction of unapproved modifications into the production environment. Furthermore, at a minimum, the banking corporation should consider such segregation for each of the following test types: unit, system integration, and user acceptance tests. Access to each environment will be granted to authorized users only, on an as-needed basis.

82. A banking corporation must establish a system development lifecycle (SDLC) management process, including for implementation of acquired systems. The banking corporation must define procedures and controls for each stage in the SDLC in alignment with said process, and ensure that it is up to date.

83. The IS and cyber defense function should be involved as applicable, in each stage of the system development lifecycle and of system implementation.

***Application Programming Interface Development***

Sections 84–91 hereinafter apply to each third party with which the banking corporation enters into an agreement in an application programming interface (API), excluding Sections 85–86, which apply exclusively to third parties to which Proper Conduct of Banking Business Directive No. 368 "Open Banking" does not apply.

84. A banking corporation must establish proper control measures for managing API development and services, to ensure the secure delivery of these services.

85. A banking corporation must implement a process that includes an assessment of the third party's suitability in connecting to the banking corporation via APIs, and an examination of its manner of access. This process must include reference, but is not limited, to the following factors: the nature of the third party's business operations, the state of the third party's IS, and the third party's reputation.

86. A banking corporation must conduct a risk assessment before allowing a third party to connect to its systems via API and must ensure that implementation of the interface is commensurate with the criticality and sensitivity of the information exchanged between them.

87. A banking corporation must establish IS principles for API design and development. These principles must include reference but are not limited to measures to protect the means of access to the APIs (such as keys or tokens) that are used to share confidential information, and to the need to limit the validity of the means of access in order to reduce the risk of unauthorized access.

88. A banking corporation must adopt strong encryption standards and access management controls in order to securely transmit sensitive information through APIs.

89. A banking corporation must examine and test its APIs with third parties, including IS aspects, before it is deployed into production, and should log the access sessions by third parties, including the identity of the party making the API connections, date and time, and the information being accessed.

90. A banking corporation must implement, in the development process, real-time monitoring mechanisms on the API interface, which will monitor the usage and performance of the interface and detect suspicious activity. The purpose is that, in the event of an incident harming the banking corporation or its customers through the interface, the monitoring mechanisms will allow the prompt revocation of the access means to the interface.

91. A banking corporation must ensure that its system is capable of handling high volumes of API call requests, and must implement measures to mitigate IS threats, including cyber threats such as DDoS attacks.

**Change management**

92. A banking corporation must establish a change management process that ensures that changes to information assets are documented, tested, assessed, reviewed, and approved before their implementation.

93. A banking corporation must take steps to carry out a risk assessment and analysis of the effects of a change on the information asset before implementing the change. Said risk assessment and analysis must include but are not limited to aspects such as IS and the implications of the change on other information assets.

94. A banking corporation must ensure that all changes are adequately tested in a test environment. The test plan must be developed and approved by the appropriate business management and technology management functions. The test results should be accepted and

signed off before the change is deployed to the production environment.

95. A banking corporation must establish a special-purpose committee that includes permanent representatives of all the key functions involved in the change management process, including the business management function and the technology management function, and the committee must approve and prioritize changes after considering the stability and security implications of the changes to the production environment, among other issues.

96. A banking corporation must perform a backup the information asset prior to the change implementation in the production environment, and must establish a roll-back plan for the information asset in the event that a problem occurs during or after the change implementation.

97. A banking corporation must establish procedures for assessing, approving, and implementing urgent changes to production, to which the ordinary change management process cannot be applied, and must define the entity authorized to approve changes of this type, in order to reduce the risk to the production environment's stability and IS.

98. A banking corporation must ensure that it maintains an audit trail of the activities performed during the implementation of the change, which facilitates investigations and troubleshooting during or after the implementation of the change.

**Key IS-related issues in IT project and change management**

99. On the key IS-related issues in technology project management and change management processes, see Sections 123–124 hereinafter on "IS in the change management process" and Section 125 hereinafter on "Secure system acquisition and development."

## Part D –Information Security and Cyber Defense Risk Management

### Chapter G: Information Security

**IS capability**

100. A banking corporation must assess the sufficiency of its IS capability in an ongoing manner and maintain IS capability that is commensurate with the size and extent of its information assets and the risks to which said information assets are subject, in such manner that enables it to continue its operations in a a sound manner. IS capability must be revised in response to changes in IS risks, including risks resulting from changes to information assets or its business environment. To this end, the banking corporation must adopt an adaptive, forward-looking approach that includes mapping and analysis of the environment, prediction and analysis of threats, and ongoing investment in resources (budgets and labor allocations), appropriate skills, and controls (prevention, detection, and response).

101. IS capability must include but is not limited to the following elements:

101.1. management of IS vulnerabilities and threats;

101.2. situational awareness, sharing of information and intelligence;

101.3. IS operations and administration;

101.4. secured architecture development and design;

101.5. security testing including penetration testing;

101.6. a system of reporting IS risks and the capability to analyze these risks;

101.7. incident detection and response, including recovery, reporting, and communications about said incidents with relevant functions;

101.8. investigation, preservation of evidence, and in-depth analysis of IS incidents;

101.9. IS assurance.

102. A banking corporation that enters into an agreement with a third party must act according to the following principles:

102.1. When entering into an agreement with a third party, a banking corporation must assess the adequacy of that party's IS, including but not limited to the sufficiency of its resources, skills, and controls. The assessment must be made according to the potential consequences of an IS incident affecting the information assets to which the third party has access. Any capability gaps identified should be addressed in a timely manner, according to its potential impact.

102.2. When entering into an agreement with a third party that enters into an agreement with another party to perform the agreement on behalf of the third party, the banking corporation must be satisfied, through an inspection, that the other party has adequate IS capability to manage the additional IS risks resulting from this arrangement.

102.3. A banking corporation that relies on certifications, attestations, and assurance of the third party's IS capability that is provided by it, must ensure their scope, quality and independence, and take steps to address any limitations identified.

**IS and Cyber Defense management framework**

103. The IS and cyber defense management framework must be commensurate with the IS risks facing the banking corporation. The framework must include all the policies, procedures, and directions related to IS, and in accordance with them shall act the board of directors, senior management, designated committees, officers, employees, including contractors and temporary employees, third parties, and the banking corporation's customers.

104. The IS and cyber defense management framework must be aligned with the banking corporation's other frameworks, such as the risk management framework and the outsourcing management framework, must take into account the relevant legal requirements, and support the planning and implementation of IS controls.

105. A banking corporation must establish an adequate IS and cyber defense management framework based on high-level core principles; These include but are not limited to: implementing multiple layers and types of controls such that if one control fails, other controls limit the impact of an information security compromise

105.1. Defense in Depth – implementation of multiple layers of defense and types of controls that create defense systems that combine organizational and human infrastructures, procedures, processes, and technologies (People, Processes, and Technologies), such that the effects of a weakness emerging in one control are limited by other controls. In in-depth deployment of the defense, the banking corporation

must take into account an analysis of IS risks and the state of its controls and its exposure to risks compared to its vulnerabilities and threats;

105.2. Least Privilege and Need to Know – the information assets must be hardened and access to them and their access must be restricted to the minimum required to achieve the business objectives;

105.3. Timely detection of IS incidents, to mimimize the impact of an IS compromise;

105.4. Secure by Design – incorporation of IS principles into the design of the information system asset;

105.5. Privacy by Design – reducing information collection and processing to the necessary minimum, from the early design stage and along the entire lifecycle of information collection and use;

105.6. Use of and access to information assets must be attributed to an individual, hardware, or software, and activity must be logged and monitored subject to Section 61.7 above, "Management of log-based audit trails". Also see Chapter J "Monitoring IT."

105.7. Error Handling – Unauthorized access to information assets or other IS compromise will not be possible even in the event of an error, whether malicious or unintentional;

105.8. Never Trust Always Verify – verification of any party before relying on it. An example of this principle is the Zero Trust model;

105.9. Segregation of duties that is enforced through appropriate allocation of roles and responsibilities;

105.10. Design of controls that enforces compliance with the IS and cyber defense policy, and reduced reliance on the human factor;

105.11. Assumed Breach – design of detection and response controls based on the assumption that preventive controls have failed;

105.12. An overall perception of the operational environment, according to which IS and cyber defense array must take into account factors such as the banking corporation's role in the financial system's supply chain, the use of general infrastructures and services (e.g., social networks), and risks stemming from the nature of the operations, versus other factors in landscape, including foreign factors, subsidiaries (in and outside Israel), third parties, and customers;

105.13. Proactive defense concept – establishing a dynamic information security array with proactive capabilities through but not limited to the following actions:

105.13.1. up-to-date mapping and analysis of the environment in which the banking corporation operates in order to detect vulnerabilities in its information assets;

105.13.2. information collection and ongoing detection and analysis of methods of attack, intentions, and activities of threat actors in cyberspace, while implementing principles of situational awareness and information sharing with other relevant entities to produce actionable information, analyze scenarios, and engage in outside-the-box thinking, which will assist in

strengthening information security and the cyber defense array, and the operational environment against potential attacks;

105.13.3. developing rapid and effective capabilities to respond to and manage an IS incident, including the totality of its aspects and across all its stages;

105.13.4. developing capabilities of deception, diversion, and delay in response to IS incidents by using special techniques and technologies (e.g., honeypots);

105.13.5. developing operational robustness and recovery capability including the capability to absorb the implications of a significant operational disruption resulting from an IS incident, without interrupting the management of critical processes and services, and rehabilitation of the business activities after a disruption has occurred to a degree sufficient to allow the banking corporation to meet its business obligations;

105.13.6. developing capabilities of debriefing, investigation, lesson learning, and knowledge retention in relation to incidents, while using legal mechanisms and cooperation with enforcement authorities, as necessary, in order to bring perpetrators to justice.

**IS and cyber defense policy**

106. A banking corporation must refer to the following issues, among others, in its IS and cyber defense policy (see Section 15 above):

106.1. the board’s and senior management's commitment and expectations;

106.2. the goals and objectives of the IS and cyber defense policy;

106.3. adjusting the policy to the legal and regulatory environment, including the need to meet accepted standards;

106.4. a description of the tools and methodologies for assessing IS risks and the manner of their use, pursuant to Chapter C "The IT Risk Management Framework (General)."

106.5. allocation of resources to implement the IS management framework;

106.6. identity management controls and logical access management controls. See Sections 116–120 hereinafter;

106.7. IS controls in various stages of the information asset lifecycle. See Sections 112–115 hereinafter;

106.8. management of technological IS solutions. See Sections 128–129 hereinafter;

106.9. an overarching IS architecture that outlines the approach for designing the IT environment (encompassing all information assets) from a security perspective, including network segmentation, end point controls, gateway design, authentication, identity management, interface controls, software engineering, and design and location of IS technology solutions and controls;

106.10. IS aspects of teleworking;

106.11. monitoring and managing IS incidents, including detection and classification of IS incidents, reporting and escalation guidelines, preservation of evidence, and event investigation;

106.12. maintaining IS when entering into agreements with third parties;

106.13. defining accepted use of information assets by employees, contractors, temporary employees, and third parties, from the perspective of IS;

106.14. IS aspects of recruitment and vetting of staff, contractors, and temporary employees;

106.15. IS roles and responsibilities, including:

106.15.1. functions in the IS risk management framework: maintenance, monitoring, compliance (policy and procedures), training, and awareness;

106.15.2. specific IS roles: CISO, system administrators;

106.15.3. responsibilities of information asset owners and end-users;

106.15.4. functions related to risk management, controls, and compliance with the IS and cyber defense management framework;

106.15.5. responsibility for reporting assessments of the effectiveness of the IS management framework;

106.15.6. functions of the business units.

106.16. physical and environmental controls; See Section 122 hereinafter;

106.17. use of cryptographic techniques and specifically data encryption; See Section 127 hereinafter;

106.18. development or configurations by end-users; See Section 130.3 hereinafter;

106.19. the banking corporation's connectivity to public networks; See Section 135.2 hereinafter;

106.20. mechanisms to assess compliance with the IS framework and its effectiveness.

107. The IS and cyber defense policy must be documented and its summary communicated to all employees and third parties, in the aspects relevant to their respective activities.

## Chapter H: Implementation of IS controls

108. To protect its information assets, a banking corporation must implement IS controls that include reference to the following:

108.1. vulnerabilities of and threats to the information asset;

108.2. the criticality and sensitivity of the information assets;

108.3. the stage at which the information asset is within its life-cycle;

108.4. minimization of exposure to severe but plausible IS scenarios.

109. If the information assets are managed by a third party, the banking corporation must review whether the IS controls in place, or planned for implementation by the third party to protect the banking corporation's information assets, are consistent with common industry controls, accepted IS controls within the banking corporation itself, and the nature of the involved information assets. Any gap that is identified should be addressed according to the risk assessment.

110. Within the review described in Section 109 above, the banking corporation must also consider its ability, within its agreement with the third party, to review the IS controls implemented by other entities that are used by the third party to perform its obligations according to the agreement for the banking corporation.

**Identification, assessment, and implementation of controls commensurate with IS vulnerabilities and threats**

111. A banking corporation must execute an ongoing process to identify and assess existing and emerging vulnerabilities and threats pertaining to critical and sensitive information assets, including information assets that may expose critical and sensitive information assets to vulnerabilities or threats, and must apply appropriate controls to mitigate these threats. To this end, the banking corporation is required to actions that include but are not limited to the following:

    111.1. perform said process in accordance with internal and external changes, including business, organizational, technological changes and changes in the vulnerabilities and threats landscape;

    111.2. develop remediation activities for the control environment (prevention, detection, and response) that are commensurate with the threat;

    111.3. implement mechanisms that allow rapid access to intelligence from internal and external sources, and rapid analysis of information related to vulnerabilities, threats, attack methods, and countermeasures. The threat and vulnerability landscape shall 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; weaknesses, system configurations or vulnerabilities that could be exploited for attacks; attacks that occurred in the past (at the banking corporation and/or in its operational environment); response actions taken in the past, methods and indicators for detecting and identifying attacks and methods of coping with attacks ;

    This information shall be used as the basis for informed decision making, prioritizing of actions, and maintaining real time effective defense;

    111.4. share information related to threats and means of defense against them with the banking corporation's stakeholders, including government agencies, entities in the financial system, and customers, as necessary and to the greatest extent possible. Information collection and sharing is subject to the law including the instructions of the Supervisor of Banks;

    111.5. implement mechanisms that disrupt the various phases of an attack against the information assets (examples of attack phases include reconnaissance, vulnerability exploitation, malware installation, privilege escalation, and unauthorized access).

**IS controls in the information asset life cycle**

112. A banking corporation must implement security controls to protect its information assets in a manner that is commensurate with, but not limited to the stage at which the information assets are within their life-cycle. The banking corporation must ensure the effectiveness of the security controls for each stage in the lifecycle of the information assets, and assess their integrity in an ongoing manner. At a minimum, an information asset's life cycle includes the following stages: planning and design, acquisition and implementation, support and maintenance, decommissioning and destruction.

113. A banking corporation must implement planning and design controls at the first phases of the lifecycle in order to ensure that IS is incorporated within the information assets. The solutions to be implemented must be commensurate with the IS requirements stated in the IS management framework.

114. A banking corporation must implement acquisition and integration controls to ensure that IS is not compromised by the introduction of new information assets, whether through acquisition or through development, and must implement ongoing support and maintenance controls to ensure that information assets continue to meet the IS requirements of the banking corporation. These controls must address but are not limited to the following areas:

    114.1. change management—controls that address information security as part of the change management process and update the information asset inventory in an ongoing manner; see additional information in Sections 123–124 hereinafter, "IS in the change management process" and Section 125 hereinafter, "secure system acquisition and development."

    114.2. configuration management—controls that ensure that the configuration of the information assets minimizes vulnerabilities and is defined, assessed, registered, and maintained even when new vulnerabilities and threats are discovered (also see Section 61.2 above, "Configuration management").

    114.3. deployment and environment management—controls that ensure that the development, test, and production environments are appropriately segregated and secured, and assist in enforcing a segregation of duties; See additional information in Chapter F hereinabove, "Project Management and Change Management."

    114.4. Access management controls — these controls ensure that only authorized users, software, and hardware are able to access the information assets. For additional information see Sections 116–120 hereinafter, "Identity and logical access management controls."

    114.5. hardware and software asset controls — controls that prevent security breaches caused by unauthorized hardware and software assets that were incorporated into the banking corporation's IT;

    114.6. network design — controls that ensure that only authorized traffic flows through networks and that reduce the impact of security breaches;

    114.7. vulnerability management controls — controls that ensure that IS vulnerabilities are identified and handled quickly, and according to the risk assessment;

114.8. patch management controls — to assess patches and other updates that address known vulnerabilities and implement them in a timely manner (for additional details see Section 61.4 above "Patch management");

114.9. monitoring controls — that rapidly detect compromises to information security;

114.10. response controls — to manage information security incidents (for additional information see Chapter K "Incident and Problem Management");

114.11. capacity and performance management controls — that ensure that availability is not compromised by current or expected business operations. See additional information in Section 61.6 "Capacity and performance management";

114.12. service provider management controls — that ensure that these services meet the banking corporation's IS requirements;

114.13. continuous control monitoring — controls that continuously ensure the proper operation of the implemented IS controls.

115. A banking corporation must implement specific decommissioning and destruction controls to ensure that IS is not compromised when information assets reach the end of their lifecycle. These controls include but are noted limited to archiving and deleting sensitive data before the disposal of the information asset. For details see Section 61.8 hereinabove "Disposal of data and media."

**Identity and logical access management controls**

116. The principles for establishing identity management and logical access management controls are:

116.1. A banking corporation must establish identity management and logical access management controls; This includes establishing personal means of identification and authentication for each party that has access to an information asset as a precondition of granting access;

116.2. In exceptional situations in which it is not possible to establish personal means of identification and authentication—for example, when technological limitations prevent this, the banking corporation must implement appropriate compensating controls;

116.3. Identity management and logical access management controls must allow access to information assets only when a clear business need exists and only for as long as such need exists.

117. When granting access to an information asset, the banking corporation must take into account various aspects of risk assessment, including the user's business role, physical location, remote access, time and duration of access, patch and anti-malware status, software, operating system, device, method of connectivity, and criticality and sensitivity of the information asset.

118. A banking corporation must implement processes, such that personal means of identification and authentication:

118.1. are issued, managed, authenticated, revoked, and audited for authorized components, users, processes, and software;

118.2. are issued, delivered, operated, and replaced in a manner that makes it possible to ensure that sensitive information is not exposed in the issuance and delivery process, among other things.

119. The strength of identification and authentication would be commensurate with the impact on the banking corporation and its customers, should an identity be falsified. Without detracting from the generality of the above, authentication shall be of increased strength (e.g., multi-factor authentication) in the following cases, commensurate with the relevant risk assessment:

119.1. system administrator access, or access by another user with elevated privileges, to a critical or sensitive information asset ;

119.2. remote access to a critical or sensitive information asset through a public network;

119.3. activities classified as high-risk activities, pursuant to principles approved by the board of directors.

120. Notwithstanding the provisions of Section 119 hereinabove, customers who use E-banking services, as this term is defined in Proper Conduct of Banking Business Directive No. 367 on "E- Banking," are subject to the relevant provisions of said Directive and not the provisions of this Directive.

**Minimizing exposure to severe yet plausible scenarios**

121. A banking corporation shall review severe but plausible IS incidents that may affect it financially or otherwise (e.g., reputational damage or noncompliance with regulatory requirements) and potentially threaten the banking corporation's business operations. This review will help it identify and implement additional controls to prevent or reduce the impact of scenarios that include but are not limited to:

121.1. malicious acts by an attacker from within the banking corporation, with highly privileged access, who is assisted by internal or external parties;

121.2. deletion or corruption of data in both the production and the backup environments, either through malicious intent, user error, or system malfunction;

121.3. loss of or unauthorized access to encryption keys that safeguard extremely critical or sensitive information assets.

**Physical access and environmental controls**

122. A banking corporation must ensure that physical and environmental access controls are defined, documented, and implemented in order to protect its installations, including its offices and its data centers, including those managed by third parties, against unauthorized access and environmental risks. Among others, the controls shall address the following issues:

122.1. Determining the location and building facilities that provide a level of protection from natural and man-made threats. In the event of such threats, the controls shall also include reference to the diversification of access to sources that provide essential

services to installations, such as power and telecommunications, as well as fall-back mechanisms for these services that enter into operation immediately (e.g., generators, Uninterrupted Power Supply [UPS] devices);

122.2. Restricting access of employees, including contractors, temporary employees, third parties, and visitors to various areas, such as the installation, the data room, the computing racks, according to their roles and areas of responsibility. Access authorization must be reviewed periodically in order to ensure rapid revocation of authorizations that are no longer needed;

122.3. Maintaining environmental conditions such as ventilation, air conditioning and fire suppressant systems (environmental controls) within predefined parameters. These controls should be implemented according to the significance of the installation and the criticality and sensitivity of the activities and information systems located therein; and

122.4. Installing detection and alert systems that detect IS incidents where physical and environmental controls have failed. Examples of controls are sensors/alarms for volume, temperature, water, humidity, smoke, and service availability (e.g., power outages, telecommunication issues).

**IS in the change management process**

123. A banking corporation shall implement controls in the information asset change management process, including changes in hardware, software, data, and configuration, whether planned or made in response to an emergency, with the goal of ensuring that IS is maintained.

124. These controls should include, but are not limited to:

124.1. security testing to identify vulnerabilities and confirm IS requirements have been met. The nature of testing would be commensurate with the scope of the change made and the sensitivity and criticality of the impacted information asset;

124.2. segregation of duty controls in order to prevent personnel from deploying their own software changes in the production environment;

124.3. changes developed and approved in another environment sufficiently segregated from the production environment, so as to avoid any compromise of IS;

124.4. In the matter of emergency changes to which the ordinary change management process cannot be applied — see Section 97 above;

124.5. validation that IS requirements are met before the change is deployed to production, pursuant to the risk assessment;

124.6. use of dummy data for development or testing purposes, and, where essential, use of desensitized production data (e.g., deletion of names and ID/CN numbers) subject to obtaining approval from the appropriate functions in the banking corporation;

124.7. minimization to the greatest extent possible, implementation of compensating controls as much as possible, and obtaining advance approval from the appropriate authority, in case of changes that knowingly introduce security vulnerabilities that cannot be handled.

**Secure system acquisition and development**

125. A banking corporation shall implement secure system development and acquisition processes to assist in maintaining confidentiality, integrity, and availability by improving the software's quality and its vulnerability profile. The processes should, at a minimum, check the following:

    125.1. the system continues to function as intended regardless of unforeseen circumstances, including when erroneous input is entered;

    125.2. the system has a reduced propensity to be misused either intentionally or inadvertently; and

    125.3. the system complies with the banking information's IS policy framework requirements.

**Controls over means that potentially expose sensitive information**

126. A banking corporation shall implement controls over access to means that enable unauthorized disclosure of sensitive information, including as a result of human error, the outcome of which is loss of information confidentiality (hereinafter "data leakage controls"), as follows:

    126.1. A banking corporation shall grant access to means that enable removal, duplication, dissemination, or other disclosure of sensitive information based on the risk assessment and only where a valid business or operational need exists;

    126.2. A banking corporation shall implement technological and processed data leakage controls commensurate with the criticality and sensitivity of the information, where sensitive information is at risk of leakage. These controls include but are not limited to:

        126.2.1. existence of a process for granting access to information transfer mechanisms and devices, including registration and periodic review of users. Users with authorized access to sensitive information must be subject to increased scrutiny;

        126.2.2. appropriate blocking, filtering, and monitoring of electronic transfer mechanisms, websites, and printing devices;

        126.2.3. appropriate encryption (see Section 127 hereinafter, "Use of Cryptographic Techniques"), cleansing of transfer devices and means after use, and creating an audit trail over the devices;

        126.2.4. appropriate segmentation of data, based on sensitivity and access needs;

        126.2.5. existence of a monitoring process to identify unauthorized software and hardware (e.g., key loggers, password cracking software, wireless access points).

**Use of cryptographic techniques**

127. A banking corporation shall implement cryptographic techniques (methods used to encrypt data, confirm its authenticity, and verify its integrity) according to the following principles:

127.1. A banking corporation shall use cryptographic techniques to control access to its data in motion and data at rest that were classified as highly critical and highly sensitive, both on private and public networks, or networks on which the banking corporation is unable to enforce its IS and cyber defense policy. The cryptographic technique and its robustness shall be established on the basis of the criticality and sensitivity of the data, the nature of the operations, and the existence of supplementary controls, among other things, provided that an encryption technique is used. Notwithstanding the above, regarding data at rest located in the banking corporation's internal network, a data encryption technique shall be used in those cases in which it is required by the IS policy on data encryption.

127.2. In the matter of data (in motion or at rest) that is not classified as highly sensitive and highly critical:

127.2.1. On public networks or networks on which the banking corporation is unable to enforce its IS and cyber defense policy, data shall be transmitted using, at minimum, accepted encryption techniques as described in Section 127.4 hereinafter.

127.2.2. On private networks—the use of cryptographic techniques to restrict access to these data shall be established pursuant to a risk assessment that considers the criticality and sensitivity of the data, the nature of the operations, and supplementary controls, among other things.

127.3. A banking corporation must encrypt the network traffic (private or public networks or networks on which the banking corporation is unable to enforce its IS and cyber defense policy) according to a risk assessment that considers the criticality and sensitivity of the transmitted data, the nature of the operations, and supplementary controls, among other things.

127.4. Cryptographic techniques must be selected from accepted international standards and reviewed periodically to ensure that they remain commensurate with relevant vulnerabilities and threats.

127.5. The provisions of Sections 127.1–12.7.3 hereinabove will not apply in the following issues, and the relevant provisions in the following Directives will apply:

127.5.1. the requirements and exclusions in the matter of encryption in Directive no. 367 on "E-Banking";

127.5.2. the arrangement described in provision 33 of Directive 362.

127.6. A banking corporation shall establish sound cryptographic key management controls, including generation, distribution, storage, renewal, revocation, recovery, archiving, and destruction, with the aim of reducing the risk of a security compromise of the cryptographic keys.

127.7. A banking corporation shall define controls to limit access to cryptographic keys.

**Information security technology solutions**

128. A banking corporation shall implement technology solutions to protect the security of the

various information assets. These solutions include but are not limited to firewalls, network access controls, intrusion detection/prevention (IDS/IPS) systems, anti-malware, content filtering, encryption and monitoring/log analysis tools.

129. The degree of implementation of lifecycle controls on technology solutions shall be commensurate with the reliance on these solutions for IS. Lifecycle controls should include but are not limited to:

    129.1. guidelines that outline the cases and conditions in which each IS technology solution should be used;

    129.2. documents containing the objectives and requirements of each technology solution;

    129.3. authorization of individuals who may make changes to the technology solutions, taking into account the principle of segregation of duties;

    129.4. regular assessment of the technology solutions' configuration, to assess effectiveness and detect unauthorized modifications;

    129.5. periodic review of accepted industry practices; and

    129.6. implementation of mechanisms that generate an alert if the technology solutions are not working as designed.

**End-user developed software**

130. A banking corporation shall implement principles for software development by the banking corporation's end-users, including:

    130.1. A banking corporation shall define processes to detect cases of software development or configuration by end-users and to assess exposure to risks in such cases;

    130.2. End-user development or configuration of software that constitutes an information asset that is critical for the achievement of its business objectives or that processes sensitive information or data, shall comply with relevant lifecycle management controls. The banking corporation shall manage appropriate documentation of such information assets.

    130.3. A banking information shall define an end-user development or configuration policy that outlines, among other things, the cases in which development or configuration by end-users is permitted as well as the banking corporation's expectations regarding lifecycle management controls, including controls related to IS, development, change management, and backups.

**Legacy systems**

131. An information asset that was incorporated before the existing IS management framework was adopted and does not comply with its requirements should be replaced or addressed pursuant to the exemption handling policy from the IS management framework determined by the banking corporation.

**Emerging technologies**

132. A banking corporation must put principles into effect regarding the use of emerging technologies in the banking corporation, which include but are not limited to:

132.1. The use of emerging technologies in the production environment must comply with the instructions for new products in Directive no. 310, provided that one of the following conditions obtain:

132.1.1. the technology has matured to a state where there is a generally agreed set of industry-accepted controls to manage the security of the technology; or

132.1.2. compensating controls are sufficient to reduce residual risk within the banking corporation's risk appetite (e.g., segregation of networks).

132.2. Notwithstanding the above, a banking corporation that wishes to consider an emerging technology that does not meet the requirements outlined in Section 132.1 above may do so subject to the following conditions:

132.2.1. The banking corporation develops a clear, holistic, and appropriate approach to adopting innovation in its operations;

132.2.2. The banking corporation identifies and assesses the risks stemming from the emerging technology and ensures that appropriate control processes exist and are commensurate with these risks;

132.2.3. The banking corporation uses a controlled environment to examine the technology, with restrictions on the scope of operations and the number of customers, and informs the customers about the examination of the emerging technology and the potential implications for them.

**Telework**

133. A banking corporation must ensure that remote employees' access to the information assets is possible only from devices that comply with the principles and meet the requirements defined in the information security management framework, including with respect to encryption, access controls, and data leakage, and such remote access is subject to appropriate training.

134. Removal and use of print-outs outside the banking corporation's premises by employees, including contractors and temporary employees, is subject to the provisions of proper Conduct of Banking Business Directive No. 356 "Removal of Documents from the Offices of the Banking Corporations" and compliance with all the principles and requirements defined in the IS and cyber defense management framework on this matter, including on the matter of data leakage prevention.

**The banking corporation's connectivity to public networks**

135. The banking corporation's connectivity to public networks shall be carried out in accordance with the the following principles:

135.1. A banking corporation must define appropriate mechanisms to protect its online presence, specifically in view of the risks entailed in its social network activities;

135.2. A banking corporation's management must define the banking corporation's policy for connectivity to public networks based on an appropriate risk assessment and application of appropriate means of control, as outlined in Sections 128–129 hereinabove.

## Chapter I. Assessing the effectiveness of IS controls

136. A banking corporation shall map the implemented IS controls and continuously assess the level of maturity, the effectiveness of the design, implementation, and operation of said controls, through a systematic testing program.

137. A banking corporation shall develop principles for determining testing scope and frequency, including:

137.1. The frequency and scope of testing would ensure that a sufficient set of the banking corporation's IS controls are tested at least annually, and all controls are tested at least once in three years, in order to validate that IS controls remain effective. Furthermore, the testing program shall consider the criticality and sensitivity of the information asset and the potential consequences of IS incidents on the information asset, among other things.

137.2. Without detracting from the provisions of Section 137.1 hereinabove, a banking corporation shall perform a test to assess the effectiveness of the design, implementation, and operations of the controls in the event of a material change in the vulnerabilities of and threats to the information asset, a change to the information asset or the technological environment in which it operates, and before a new information asset is entered into use.

137.3. Without detracting from the provisions of Section 137.1 hereinabove, controls related to information assets exposed to environments in which the banking corporation is unable to enforce its IS and cyber defense policy must be tested throughout the year.

138. A banking corporation shall develop principles for determining the type of tests to be performed and principles for handling their results:

138.1. A banking corporation shall define the types of tests required pursuant to the type of reviewed control, of a range of accepted tools in this field, taking into account the following considerations, among others: the rate at which vulnerabilities and threats change, the criticality and sensitivity of the information asset, the consequences of an IS incident, and the materiality and frequency of changes to information asset. Examples of tests are: gap analysis against accepted information security standards, compliance review, source code review, vulnerability assessments, controlled penetration testing, and "red team" tests.

138.2. A banking corporation shall define in advance the success criteria for tests, including the circumstances that require re-testing.

138.3. Test results must be reported to senior management together with recommended remedial action. Senior management must complete its discussions on the test findings and their implications and make the required decisions, including the determination of a schedule for their implementation. Senior management shall formally track the implementation of these decisions. The entire process shall be carried out within a reasonable time after the commencement date of the testing process.

138.4. Material findings that emerged from the tests, and any finding that indicates a

deficiency in IS controls and that cannot be remediated in a reasonable timeframe shall be brought to the attention of the board of directors or the appropriate board committee. The reasonable timeframe for correcting a finding shall be determined on the basis of the nature of the finding, and the criticality and sensitivity of the information asset in relation to which the information security control is implemented, among other things.

139. The tests shall be performed by parties with the appropriate knowledge, expertise, and skills to conduct the tests, who are independent and not involved in the operations and the activation of the controls being tested, in order to prevent conflicts of interest. The degree of their independence shall be determined according to the type and significance of the test that is being conducted, among other things.

140. Where the banking corporation's information assets are managed by a third party, and the banking corporation is reliant on that party's information security control testing, the banking corporation shall assess whether the frequency and type of testing of controls in respect of those information assets are determined on the basis of the principles outlined in Sections 137–138.1 and 139 hereinabove. The banking corporation shall assess the impact of each deficiency found on its ability to continue to use the third party's services.

## Part E – Incident Management

### Chapter J – Monitoring IT

141. A banking corporation must establish policies and procedures to detect emerging problems or anomalous activities and prevent them from evolving into technological failures incidents or IS incidents (hereinafter in this part, "incidents"), understand the nature of the incidents, cope with incidents, reduce their impact, and support investigations of incidents (also see Chapter K "Incident Management"). As part of this continuous monitoring activity, a banking corporation shall implement appropriate and effective capabilities for detecting and reporting breaches of confidentiality, integrity, or availability of the information assets, and for detecting physical or logical intrusions. The continuous monitoring and detection processes should also cover the following issues:

141.1. anomalies in technology (system operations and performance – command and control) and in business operations;

141.2. transactions - to detect misuse of authorizations by third parties or other entities in or outside the banking corporation;

141.3. relevant internal and external factors, including business and IT administrative functions;

141.4. potential internal and external threats.

142. A banking corporation shall establish processes and an organization structure to identify and constantly monitor IT risks that could materially affect its ability to provide services. Within these actions, the banking corporation must:

142.1. maintain an effective monitoring and control system, staffed continuously

(24×7×365); receive reports from the various systems in real time, including from the operational and business systems; identify indicators of incident occurrence; and initiate reporting and response activities as necessary;

142.2. continuously review the evolving nature of the threat landscape and the accepted practices for monitoring and detecting them, and from time to time review information security incident scenarios, in order to assess its ability to detect them, and update the monitoring and detection processes and tools accordingly;

142.3. implement means of identifying the materialization or potential materialization of information security risks such as potential data leakage, malicious code, and other IS threats, and software and hardware vulnerabilities, and shall review appropriate responses (e.g., through new security updates).

143. The monitoring systems must be integrated with other systems in the banking corporations to enable an effective process of incident detection and handling, including identification of indicators of anomalous activities and trends, data recovery and enrichment, investigation and documentation, knowledge management and decision making, creating and managing alerts and reports, communications with relevant entities, and real time system modifications.

## Chapter K – Incident and problem management

### General

144. A banking corporation shall implement an incident management process to monitor and log technological failure incidents and information security incidents. The incident management process shall enable the banking corporation to continue or resume secure and stable operations of the affected functions and processes as soon as possible, such that the incident's impact on the banking corporation's business operations and on its customers is minimal.

145. To minimize the impact of adverse events and enable rapid recovery, a banking corporation shall establish appropriate processes and organizational structures (hereinafter, "the incident management framework") that ensure that:

145.1. actions, monitoring, and handling are consistent and integrated;

145.2. the root causes are identified and eliminated to prevent the occurrence of repeated incident.

146. The incident and problem management framework shall address, among other things, the following issues:

146.1. the procedures for identifying, diagnosing, logging, and classifying incidents according to the criticality and sensitivity of the affected business process;

146.2. maintenance and protection of information related to the incident in order to conduct an investigation of the incident and identify its root cause;

146.3. the roles and responsibilities of employees and external parties in monitoring, analyzing, escalating, decision making, resolution, and recording, in different incident scenarios (e.g., errors, malfunctions, cyber attacks);

146.4. allocation of appropriate resources to employees for the purpose of performing their duties and responsibilities;

146.5. problem management procedures to identify, analyze, and solve the root cause behind one or more incidents - The banking corporation should analyze incidents that affected or had the potential to affect the banking corporation and have been identified or have occurred within or outside the banking corporation, and trends in their occurrence, consider key lessons learned from these analyses and accordingly determine if preventive or remediation activities are necessary;

146.6. an appropriate system of internal reporting to entities within the banking corporation, including procedures for reporting incidents and escalation criteria that also consider security-related customer complaints, to ensure that:

146.6.1. incidents with a potentially high adverse impact on critical and sensitive information assets are reported to senior management. IT senior management, and other relevant internal entities;

146.6.2. the board of directors is immediately informed of an occurrence of a significant incident, where such reports include the following, at minimum: the impact of the incident, the response, and aadditional controls to be implemented in order to handle the incident.

146.7. incident response procedures to mitigate the impacts related to the incident and to ensure that the service becomes operational and secure as soon as possible, and integration of these procedures with business continuity processes including the BCP;

146.8. a plan to review and test the banking corporation's response plans for information security incidents and technology failure incidents, to be conducted at least once a year for each type of incident. To ensure the effectiveness of the response plans and that fit this purpose:

146.8.1. the banking corporation's review and exercise plan shall include but is not limited to exercises by the banking corporation's various response arrays, taking into account the various types of tests (simulations of various types of technology failures, attacks, war games, etc.) and with reference to the relevant entities involved (e.g., technical entities, crisis management teams, decision makers, spokespersons, etc.);

146.8.2. A banking corporation shall establish in advance success criteria of the exercises, including the circumstances in which a repeat exercise is required;

146.8.3. The results of the exercise and a schedule for implementing the decisions made to correct the deficiencies, shall be reported to the appropriate entities that will track the implementation thereof.

146.9. external communication plans for critical functions and business processes, that include but are not limited to the following issues:

146.9.1. collaboration with relevant stakeholders in the banking corporation and

other relevant entities in order to effectively respond to and recover from the incident;

146.9.2. updates to external parties (e.g., customers, other market participants, various regulatory authorities), as appropriate and in line with applicable regulation;

146.9.3. management of the communication aspects of the incident.

146.10. cooperation and coordination with third parties on the following issues, according to the criticality and sensitivity of the information asset:

146.10.1. A periodic exercise by the third party of its response plans for incidents related to the banking corporation's information assets managed by said third party;

146.10.2. agreement on the roles and responsibilities of each party in response to an incident that requires multi-party cooperation and coordination, including agreement on the interface between the banking corporation's response plans and those of the third party, and the third party's involvement in the banking corporation's periodic exercise;

146.10.3. coordination between the banking corporation's response plans and the third party's business continuity processes, including its BCP.

**IS incidents**

In addition to the provisions set forth in Sections 141–146 above, the following further requirements shall apply with respect to information security incidents:

***Information security incident response and management***

147. When managing an information security incident, a banking corporation shall identify the current stage of the incident, and handle it according to its features:

147.1. Detection – perform a preliminary investigation of the occurrence of the security incident and determine the mode of operation required for the subsequent stage as quickly as possible;

147.2. Analysis – perform an in-depth investigation of the information security incident, in the most comprehensible and thorough manner as possible, in order to make actionable decisions, develop a list of potential alternative actions to stop the event, and decide on the main mode of action for the containment stage;

147.3. Containment – establish preliminary control of the information security incident in order to contain it and stop it from escalating and achieving its objectives, gain control over the cause of the incident, including the attack vectors, within the banking corporation, and completely stop the damage vector;

147.4. Eradication – neutralize the causes of the information security incident, including the attack components located in the banking corporation's systems, with the aim of remedying or mitigating the damage caused, to the greatest extent possible;

147.5. Recovery – return to full and proper operations by the banking corporation in each

activity affected by the information security incident that compromised its IS and restricted, disrupted, or caused the cessation of its operations.

148. A banking corporation shall establish reporting, management, response, and post-incident procedures, and procedures regarding information security incident alerts from a reliable source, whether an incident is anticipated, has occurred, or is currently occurring but before it is detected by the banking corporation, according to the severity of the incident and the stage of the response.

149. A banking corporation shall set up a situation room for the purpose of information security incident management, and define, from an integrated, corporate-wide perspective, the situation room's staff, their duties and authorities, internal and external reporting entities, modes of communication, work tools, and detailed work procedures.

150. A banking corporation shall record and monitor in an orderly manner information security incidents that were handled and the actions taken by relevant functions. Specifically, the banking corporation shall maintain an "incident log" documenting all the notifications, decisions, and actions taken in reference to a information security incident, as soon as possible after its occurrence.

151. A banking corporation shall define a pool of response activities (e.g., configuration changes, restriction and/or diversion of communications, software deployment) in accordance with various scenarios, and define the conditions in which these response activities will be performed, their specific mode of performance, the individuals authorized to order their performance, the communication channels and required authorizations, and assessment of the response's effectiveness in the specific information security incident in which it was applied.

152. A banking corporation shall define a scale of alert levels and the required activities in accordance with various alerts and scenarios, such as: prediction of an organized attack; the volume and severity of detected attacks within the banking corporation, the banking sector or the nation; detection of a material weakness or identification of attack tools that constitute a direct threat to the banking corporation.

## Part F – Miscellaneous

### Chapter L – Reporting IT and IS Risks

153. The regular reports submitted to management and the board of directors concerning operational risks, as required by Directive 350, shall include detailed reference to IT risks and IS risks.

154. IT risk reports and IS risk reports must include, but are not limited to:

154.1. use of operational metrics to identify IT risks in IT operations;

154.2. use of qualitative and quantitative assessment metrics to quantify the exposure to IS risks such that it is possible to monitor the changes in these values over time;

154.3. deviations from risk appetite and non-compliance with risk thresholds, limits, or quantitative requirements established for IS risks;

154.4. details of IS incidents and technology failure incidents according to criteria defined by the banking corporation, including an analysis of the causes of those incidents;

154.5. relevant external events and data, including regulatory changes, that potentially affect the banking corporation.

## Chapter M – Third-Party Risk Management (TPRM)

155. A third party may be the source of some of the IT risks to which the banking corporation is exposed (e.g., supply chain risks). Therefore, this Directive includes specific requirements concerning various topics, for managing those risks, which are in addition to the prudential requirements related to outsourcing in Directive 359A and Directive 362. See Appendix "Instructions for Third-Party Risk Management".

## Chapter N – Business Continuity Management (BCM)

156. The meanings of the terms in this chapter that also appear in Directive 355 shall be the meanings ascribed to them in Directive 355 on "Business Continuity Management."

157. A banking corporation shall establish appropriate technological processes pursuant to this chapter, to support the BCM process to be established according to Directive 355.

**Business impact analysis (BIA)**

158. A banking corporation shall ensure that its information systems and technological services are planned in alignment with and adjusted to the business impact analysis in Directive 355.

**Business continuity planning (BCP)**

159. The business continuity plan should take into consideration risks that may adversely impact the information systems or the technological services. The plan should support protection of confidentiality, integrity, and availability of the business activities, the supporting processes, and the information assets, and support their recovery after being compromised, as necessary. A banking corporation shall establish a business continuity plan in coordination with relevant internal and external stakeholders, as necessary.

160. A banking corporation shall establish the business continuity plan to ensure that it is able to react appropriately to potential failure scenarios and recover the operation of its critical processes and services in the event of a disruption, within a recovery time objectives (RTO) and recovery point objectives (RPO). In case of a severe operational disruption that triggers specific business continuity plans, a banking corporation should prioritize business continuity actions using a risk-based approach that can be based on, among other things, the risk assessment performed according to Section 46 hereinabove.

161. In its business continuity plan, the banking corporation should consider a range of various scenarios to which it may be exposed, including severe but plausible scenarios, and cyber-attack scenarios, and should assess their potential impact on its critical processes and services. Based on these scenarios, the banking corporation should describe how continuity of information systems and technological services, as well as its IS, are ensured.

**Disaster recovery plan (DRP)**

162. A banking corporation shall prepare a disaster recovery plan (DRP) based on the BIA and the severe but plausible scenarios described above. The DRP should specify what conditions may prompt activation of the plan, what actions should be taken to ensure the availability, continuity, and recovery of the information systems and technological services that support the banking corporation's critical processes and services. The DRP must be aligned with the recovery objectives of the banking corporation's operations.

163. The DRP should consider both short-term and long-term recovery options. The plan should be:

    163.1. focused on the recovery of the operations of the critical processes and services, supporting technological processes and information assets and their interdependencies, in order to avoid adverse effects on the functioning of the banking corporation and the banking system.

    163.2. documented and made available to the business units and the technological units, and accessible during an emergency;

    163.3. updated with and take into consideration lessons learned from incidents, tests, and exercises; new risks identified; and changes in the BIA, the recovery objectives, and recovery priorities.

164. The DRP should include reference to alternative options where recovery may not be feasible in the short term because of costs, risks, logistics, or unforeseen circumstances.

165. The DRP should include continuity measures to be implemented in order to mitigate failures of third parties that have a significant impact on the functioning of the banking corporation's IT (pursuant to the instructions in the matter of critical suppliers and service providers in Directives 355, 359A, and 362, as relevant to each specific third party).

**Disaster recovery plan testing**

166. Banking corporations must test their DRP for technological processes and information assets that support critical processes and services, and their interdependencies, at least annually.

167. DRPs must be updated at least annually, based on test results, current threat intelligence, and lessons learned from previous events. Reference must be made to each change in the recovery objectives, the recovery time, or each change in the critical processes and services, the supporting technological processes, and the supporting information assets, as necessary.

168. A banking corporation’s testing of its DRP should demonstrate its ability to sustain the viability of its businesses until critical processes and services are re-established. To this end, these tests must include the following features, at a minimum:

    168.1. an adequate set of tests of severe but plausible scenarios including those considered for the development of the BCP (as well as testing of services provided by third parties, where applicable). The set of tests should include a test of the switch-over of supporting technological processes and information assets that support critical business functions to an alternative solution that supports the banking corporation's functional continuity (e.g., a test of the switch-over from the main computer site to

an alternative solution in the event of a failure in the main computer site), and a test that demonstrates that the banking corporation is able to operate in this manner for the appropriate period and then resume normal functioning;

168.2. be designed to challenge the assumptions on which the DRP rests;

168.3. include procedures to verify that their staff and contractors, information systems and technological services are able to respond adequately to the scenarios defined in Section 168.1 hereinabove.

169. Test results should be documented, and identified deficiencies resulting from the tests should be analyzed, addressed, and reported to senior management and the board of directors.

## Chapter O: Foreign Banks

170. The Directive shall apply to foreign banks, with the following exceptions:

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

170.2. The following paragraph will be added to Section 61.5: "A foreign bank shall at all times retain in the local information systems at its branches in Israel full data containing all the personal and administrative particulars as to the owners of the accounts, the legal representatives and the signatory rights and also all the current balances of the accounts being conducted at its branches in Israel."

170.3. The following paragraph will be added to Section 138.4: "An executive summary of the testing results, together with recommendations for remediation activities, must be submitted to the officer in charge of cyber defense and information security in the parent bank."

## Chapter P: Reporting to the Banking Supervision Department

171. A banking corporation must report to the Supervisor of Banks on the following issues and events:

171.1. Technological failure incidents and IS incidents, pursuant to the requirements of Proper Conduct of Banking Business Directive No. 366 on "Reporting of Technological Failure and Cyber Incidents."

171.2. The appointment and anticipated departure of a CTO, as described in Section 26 above, or the appointment and anticipated departure of a CISO, as described in Section 34 above.

171.3. The appointment for a period of more than one month of an acting CTO, as described in Section 26 above, and an acting CISO, as described in Section 34 above.

171.4. A decision to make substantial modifications to the IT management strategy or policy, a significant conversion of the computing systems, or re-computerization of central systems and their like.

**Revisions**

| Circular No. | Details | Version | Date |
|---|---|---|---|
| 2799 | Original circular | 1 | November 18, 2024 |

**Appendix – Instructions for Third Party Risk Management**

Instructions on various issues related to third party risk management appear throughout this Directive, including:

1. The board of directors' duty to also consider, in all its discussions, issues arising from the banking corporation's reliance on third parties to manage its information assets. See Section 18 hereinabove.
2. Implementation of an identification and mapping process for each of the banking corporation's information assets, including those managed through third parties. See Section 43.2 hereinabove.
3. An information security training and awareness program. See Section 53 above.
4. The operational resilience of the cloud computing environment used to provide critical actions to the banking corporation's customers. See Section 56.2 above.
5. The banking corporation's technology infrastructure managed by a third party. See Section 58.1 above.
6. The backup process. See Section 61.5.3 above.
7. Capacity-related issues. See Section 61.6.6 above.
8. Transit of log files. See Section 61.7.5 above.
9. Arrangements to delete the banking corporation's data stored with third parties. See Section 61.8.3 above.
10. The IT planning and investment process. See Section 64.2 above.
11. The system acquisition management process. See Sections 75–78 above.
12. API development. See Sections 84–91 above.
13. Assessment of information security capability. See Section 102 above.
14. The information security and cyber defense management framework. See Section 103 above.
15. The information security and cyber defense policy. See Sections 106.12–106.13 and 107 above.
16. Implementing security controls on information assets managed by third parties. See Sections 109–110 above.
17. Third party service management controls that ensure compliance with the banking corporation's information security requirements. See Section 114.12 above.
18. Physical and environmental access controls. See Section 122 above.
19. Assessing the effectiveness of the controls of information assets managed by third parties. See Section 140 above.
20. Cooperation and coordination with third parties upon the occurrence of an incident. See

Section 146.10 above.

21. DRP. See Section 165 above.

22. DRP testing. See Section 168.1 above.

This list is presented for the reader's convenience. In the event of a contradiction between this Appendix and the provisions of the Directive, the provisions of the Directive prevail.