BANK OF GREECE

EUROSYSTEM

THE EXECUTIVE BOARD

Meeting 190/16.06.2021

Subject 2: Adoption of the guidelines of the European Banking Authority (EBA/GL/2019/04) on Information and Communications Technology (ICT) and Security Risk Management

The Executive Committee of the Bank of Greece, having regard to:

(a) Articles 28 and 55A of the Statute of the Bank of Greece (Government Gazette A298);

(b) the provisions of Law 4261/2014 "Access to the activity of credit institutions and prudential supervision of credit institutions and investment firms (transposition of Directive 2013/36/EU), repeal of Law 3601/2007, and other provisions (Government Gazette A107), in particular Articles 4 and 6, Article 66(3) and Articles 77, 102 and 153 thereof;

(c) the provisions of Law 4701/2020 "Micro-credit framework, financial sector regulation and other provisions" (Government Gazette A128), in particular Article 4 thereof;

(d) the provisions of Law 4537/2018 "Transposition of Directive (EU) 2015/2366 on payment services into Greek law and other provisions" (Government Gazette A84), in particular Articles 5, 23, 94 and 95 thereof;

(e) the provisions of Law 4354/2015 "Non-performing loans management, wage provisions, and other emergency provisions for the implementation of the agreement on fiscal targets and structural reforms" (Government Gazette A176), in particular Article 1 thereof;

(f) the provisions of Chapter A of Part 2 of Law 4021/2011 "Enhanced measures for the supervision and resolution of credit institutions — Regulation of financial matters — Ratification of the Framework Agreement on the European Financial Stability Facility and its amendments, and other provisions" (Government Gazette A218), in particular Articles 12(1) and 13 thereof;

(g) the provisions of Law 1905/1990 "Factoring contracts and other provisions" (Government Gazette A147), in particular Article 5 thereof;

(h) the provisions of Law 1665/1986 "Financial leasing contracts" (Government Gazette A194), in particular Article 2 thereof;

(I) Law 5422/1932 “Suspension of the obligation of the Bank of Greece to redeem its notes and regulation of the purchase and sale of foreign exchange” (Government Gazette A133), as in force after the insertion of paras. 3 to 6 by Article 15 Law 2515/1997 “Practice of the profession of tax accountant, operation of the Institute of Certified Appraisers (SOE) and other provisions” (Government Gazette A154), in particular Article 2 thereof;

(j) Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176/27.6.2013);

(k) Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions (OJ L 287/63/29.10.2013), in particular Articles 4 and 6 thereof and recital 28 thereof;

(l) Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing the European Supervisory Authority (European Banking Authority), amending Decision 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331/15.12.2010), in particular Article 4(2) and Article 16(3) thereof;

(m) Bank of Greece Executive Committee Act (ECA) 178/5/2.10.2020 “Outsourcing framework” (Government Gazette B4410);

(n) ECA 157/3/02.04.2019 “Adoption of the guidelines of the European Banking Authority on major incident reporting under Directive 2015/2366/EU” (Government Gazette B1646);

(o) ECA 164/2/13.12.2019 "Terms and conditions for (a) the authorisation of payment institutions and e-money institutions and for the registration of account information service providers in Greece; (b) the acquisition of, or increase in, or sale of, a qualifying holding; (c) the taking up of a post in the board of directors and other posts; (d) the stipulation of the minimum monetary amount of the professional indemnity insurance or other comparable guarantee; (e) supervisory rules; and (f) the keeping of a register under Article 14 of Law 4537/2018” (Government Gazette B4522);

(p) Bank of Greece Governor's Act 2577/2006 “Framework of operational principles and criteria for the evaluation of the organisation and Internal Control Systems of credit and financial institutions and relevant powers of their management bodies” (Government Gazette A59);

(q) the guidelines of the European Banking Authority on internal governance (EBA/GL/2017/11);

(r) the guidelines of the European Banking Authority on Information and Communications Technology (ICT) and Security Risk Management (EBA/GL/2019/04); and

(s) the fact that no expenditure shall be incurred by the Government Budget as a result of the provisions hereof,

HAS DECIDED AS FOLLOWS:

To adopt the guidelines of the European Banking Authority on Information and Communications Technology (ICT) and Security Risk Management, specifying the risk management measures to be taken, as follows:

CHAPTER I. SCOPE AND DEFINITIONS

1. The provisions of this Act shall apply to the following institutions (hereinafter referred to as “institutions”):

   a. credit institutions authorised in Greece;
   b. branches of credit institutions authorised in a non-EEA country operating in Greece;
   c. payment service providers referred to in Article 4(11) of Law 4537/2018 (hereinafter referred to as “PSPs”), authorised in Greece, in relation to the payment services referred to in Article 4(3) of Law 4537/2018 and in relation to the activity of issuing, redeeming and distributing electronic money (for the purposes of this Act, payment services are understood as the activities referred to in Article 4(3) of Law 4537/2018, as well as the activity of issuing, redeeming and distributing electronic money);
   d. leasing companies authorised in Greece,
   e. factoring companies authorised in Greece;

f. credit companies authorised in Greece;

g. credit servicing companies authorised in Greece which refinance loans, in accordance with Article 1(20) of Law 4354/2015;

h. micro-credit institutions; and

i. bureaux de change authorised in Greece.

2. The provisions of this Act shall be applied by the credit institutions referred to in para. 1(a) above on a solo basis, on a sub-consolidated and a consolidated basis in accordance with Article 102 of Law 4261/2014. The other obligated persons referred to in para. 1 above shall apply the provisions of this Decision on a solo basis.

3. This Act includes information security requirements, including cybersecurity, to the extent that information is held in ICT systems.

4. Save as otherwise specified herein, terms used and defined in Law 4261/2014, Regulation (EU) No 575/2013 and Law 4537/2018 shall have the same meaning in this Act. In addition, for the purposes of this Act, the following definitions shall apply:

Information and Communications Technology (ICT) and Security Risk

Risk of loss due to breach of confidentiality, failure of integrity of systems and data, inappropriateness or unavailability of systems and data or inability to change information technology (IT) within a reasonable time and with reasonable costs when the environment or business requirements change (i.e. agility). This includes security risks resulting from inadequate or failed internal processes or external events, including cyber-attacks or inadequate physical security.

Operational or security incident

A singular event or a series of linked events unplanned by the institution that has or will probably have an adverse impact on the integrity, availability, confidentiality and/or authenticity of services.

Control functions

The functions of the institution which are independent of the business and corporate functions whose activities and risks they control and monitor. Independent control functions typically include risk management, compliance and internal audit functions.

Risk appetite

The aggregate level and types of risk that the institutions are willing to assume within their risk capacity, in line with their business model, to achieve their strategic objectives.

ICT projects

Any project, or part thereof, where ICT systems and services are changed, replaced, dismissed or implemented. ICT projects can be part of wider ICT or business transformation programmes.

Third party

An organisation that has entered into business relationships or contracts with an entity to provide a product or service.

Information asset

A collection of information, either tangible or intangible, that is worth protecting.

ICT asset

An asset of either software or hardware that is found in the business environment.

ICT systems

ICT set-up as part of a mechanism or an interconnecting network that supports the operations of an institution.

ICT services

Services provided by ICT systems to one or more internal or external users. Examples include data entry, data storage, data processing and reporting services, but also monitoring, and business and decision support services.

CHAPTER II. PROPORTIONALITY — GOVERNANCE AND STRATEGY

1. Proportionality

5. All institutions shall comply with the provisions of this Act in in such a way that is proportionate to, and takes account of, the institutions' size, their internal organisation, and the nature, scope, complexity and riskiness of the services and products that the institutions provide or intend to provide.

2. Governance and strategy

2.1 Governance

6. The Board of Directors shall ensure that institutions have an adequate internal governance and internal control framework for their ICT and security risks. The Board of Directors shall set clear roles and responsibilities for ICT functions, information security risk management, and business continuity, including those for the Board of Directors itself and its committees.

7. The Board of Directors shall ensure that the quantity and skills of institutions' staff are adequate to support their ICT operational needs and their ICT and security risk management processes on an ongoing basis and to ensure the implementation of their ICT strategy. The Board of Directors shall ensure that the allocated budget is appropriate to fulfil the above. Furthermore, institutions shall ensure that all staff members, including key function holders, receive appropriate training on ICT and security risks, including on information security, on an annual basis, or more frequently if required.

8. The Board of Directors shall have overall accountability for setting, approving and overseeing the implementation of institutions' ICT strategy as part of their overall business strategy as well as for the establishment of an effective risk management framework for ICT and security risks.

2.2 Strategy

9. The ICT strategy shall be aligned with the institutions' overall business strategy and shall define:

a) how institutions' ICT shall evolve to effectively support and participate in their business strategy, including the evolution of the organisational structure, ICT system changes and key dependencies with third parties;

b) the planned strategy and evolution of the architecture of ICT, including third party dependencies; and

c) clear information security objectives, focusing on ICT systems and ICT services, staff and processes.

10. Institutions shall establish sets of action plans that contain measures to be taken to achieve the objective of the ICT strategy. These shall be communicated to all relevant staff (including contractors and third party providers where applicable and relevant). The action plans shall be periodically reviewed to ensure their relevance and appropriateness. Institutions shall also establish processes to monitor and measure the effectiveness of the implementation of their ICT strategy.

2.3 Use of third party providers

11. Without prejudice to ECA 178/5/2.10.2020 "Outsourcing framework", institutions shall ensure the effectiveness of the risk-mitigating measures as defined by their risk management framework, including the measures set out in this Act, when operational functions of payment services and/or ICT services and ICT systems of any activity are outsourced, including to group entities, or when using third parties.

12. To ensure continuity of ICT services and ICT systems, institutions shall ensure that contracts and service level agreements (both for normal circumstances as well as in the event of service disruption) with providers (group entities or third party providers) include the following:

a) appropriate and proportionate information security-related objectives and measures including requirements such as minimum cybersecurity requirements, specifications of the financial institution's data life cycle, any requirements regarding data encryption, network security and security monitoring processes, and the location of data centres; and

b) operational and security incident handling procedures, including escalation and reporting.

13. Institutions shall monitor and seek assurance on the level of compliance of these providers with the security objectives, measures and performance targets of the institution.

CHAPTER III. ICT AND SECURITY RISK MANAGEMENT FRAMEWORK

3.1 Organisation and objectives

14. Institutions shall identify and manage their ICT and security risks. The ICT function(s) in charge of ICT systems, processes and security operations shall have appropriate processes and controls in place to ensure that all risks are identified, analysed, measured, monitored, managed, reported and kept within the limits of the institution's risk appetite and that the projects and systems they deliver and the activities they perform are in compliance with external and internal requirements.

15. Institutions shall assign the responsibility for managing and overseeing ICT and security risks to a control function, adhering to the requirements of Bank of Greece Governor's Act 2577/2006. Institutions shall ensure the independence and objectivity of this control function by appropriately segregating it from ICT operations processes. This control function shall be directly accountable to the Board of Directors and responsible for monitoring and controlling adherence to the ICT and security risk management framework. It shall ensure that ICT and security risks are identified, measured, assessed, managed, monitored and reported. Institutions shall ensure that this control function is not responsible for any internal audit.

The internal audit function shall, following a risk-based approach, have the capacity to independently review and provide objective assurance of the compliance of all ICT and security-related activities and units of an institution with the institution's policies and procedures and with external requirements.

16. Institutions shall define and assign key roles and responsibilities, including the information security officer, and relevant reporting lines, for the ICT and security risk management framework to be effective. This framework shall be fully integrated into, and aligned with, institutions' overall risk management processes.

17. The ICT and security risk management framework shall include processes in place to:

a) determine the risk appetite for ICT and security risks, in accordance with the risk appetite of the institution;

b) identify and assess the ICT and security risks to which an institution is exposed;

c) define mitigation measures, including controls, to mitigate ICT and security risks;

d) monitor the effectiveness of these measures as well as the number of reported incidents, including for PSPs the incidents reported in accordance with Article 95 of Law 4537/2018 affecting the ICT-related activities, and take action to correct the measures where necessary;

e) report to the Board of Directors on the ICT and security risks and controls; and

f) identify and assess whether there are any ICT and security risks resulting from any major change in ICT system or ICT services, processes or procedures, and/or after any significant operational or security incident.

18. Institutions shall ensure that the ICT and security risk management framework is documented, and continuously improved, based on ‘lessons learned’ during its implementation and monitoring. The ICT and security risk management framework shall be approved and reviewed, at least once a year, by the Board of Directors.

3.2 Identification of functions, processes and assets

19. Institutions shall identify, establish and maintain updated mapping of their business functions, roles and supporting processes to identify the importance of each and their interdependencies related to ICT and security risks.

20. In addition, institutions shall identify, establish and maintain updated mapping of the information assets supporting their business functions and supporting processes, such as ICT systems, staff, contractors, third parties and dependencies on other internal and external systems and processes, to be able to, at least, manage the information assets that support their critical business functions and processes.

3.3 Classification and risk assessment

21. Institutions shall classify the identified business functions, supporting processes and information assets referred to in paras. 19 and 20 above in terms of criticality.

22. To define the criticality of these identified business functions, supporting processes and information assets, institutions shall, at a minimum, consider the confidentiality, integrity and availability requirements. There shall be clearly assigned accountability and responsibility for the information assets.

23. Institutions shall review the adequacy of the classification of the information assets and relevant documentation, when risk assessment is performed.

24. Institutions shall identify the ICT and security risks that impact the identified and classified business functions, supporting processes and information assets, according to their criticality. This risk assessment shall be carried out and documented annually or at shorter intervals if required. Such risk assessments shall also be performed on any major changes in infrastructure, processes or procedures affecting the business functions, supporting processes or information assets, and consequently the current risk assessment of institutions shall be updated.

25. Institutions shall ensure that they continuously monitor threats and vulnerabilities relevant to their business processes, supporting functions and information assets and shall regularly review the risk scenarios impacting them.

3.4 Risk mitigation

26. Based on the risk assessments, institutions shall determine which measures are required to mitigate identified ICT and security risks to acceptable levels and whether changes are necessary to the existing business processes, control measures, ICT systems and ICT services. An institution shall consider the time required to implement these changes and the time to take appropriate interim mitigating measures to minimise ICT and security risks to stay within the institution’s ICT and security risk appetite.

27. Institutions shall define and implement measures to mitigate identified ICT and security risks and to protect information assets in accordance with their classification.

3.5 Reporting

28. Institutions shall report risk assessment results to the Board of Directors in a clear and timely manner. Such reporting is without prejudice to the obligation of PSPs

to provide competent authorities with an updated and comprehensive risk assessment, as laid down in Article 94(2) of Law 4537/2018.

3.6 Audit

29. An institution’s governance, systems and processes for its ICT and security risks shall be audited on a periodic basis by auditors with sufficient knowledge, skills and expertise in ICT and security risks and in payments (for PSPs) to provide independent assurance of their effectiveness to the Board of Directors. The auditors shall be independent within or from the institution. The frequency and focus of such audits shall be commensurate with the relevant ICT and security risks.

30. An institution’s Board of Directors shall approve the audit plan, including any ICT audits and any material modifications thereto. The audit plan and its execution, including the audit frequency, shall reflect and be proportionate to the inherent ICT and security risks in the institution and shall be updated regularly.

31. A formal follow-up process including provisions for the timely verification and remediation of critical ICT audit findings shall be established.

CHAPTER IV. INFORMATION SECURITY

4.1 Information security policy

32. Institutions shall develop and document an information security policy that shall define the high-level principles and rules to protect the confidentiality, integrity and availability of institutions’ and their customers’ data and information. For PSPs this policy is identified in the security policy document to be adopted in accordance with Article 5(1)(j) of Law 4537/2018. The information security policy shall be in line with the institution’s information security objectives and based on the relevant results of the risk assessment process. The policy shall be approved by the Board of Directors.

33. The policy shall include a description of the main roles and responsibilities of information security management, and it shall set out the requirements for staff and contractors, processes and technology in relation to information security, recognising that staff and contractors at all levels have responsibilities in ensuring institutions’ information security. The policy shall ensure the confidentiality, integrity and

availability of, at a minimum, an institution's critical logical and physical assets, resources and sensitive data whether at rest, in transit or in use. The information security policy shall be communicated to all staff and contractors of the institution.

34. Based on the information security policy, institutions shall establish and implement security measures to mitigate the ICT and security risks that they are exposed to. These measures shall include:

a) organisation and governance in accordance with paras. 14 and 15 above;

b) logical security (Section 4.2);

c) physical security (Section 4.3);

d) ICT operations security (Section 4.4);

e) security monitoring (Section 4.5);

f) information security reviews, assessment and testing (Section 4.6); and

g) information security training and awareness (Section 4.7).

4.2 Logical security

35. Institutions shall define, document and implement procedures for logical access control (identity and access management). These procedures shall be implemented, enforced, monitored and periodically reviewed. The procedures shall also include controls for monitoring anomalies. These procedures shall, at a minimum, implement the following elements, where the term 'user' also includes technical users:

a) Need to know, least privilege and segregation of duties: institutions shall manage access rights to information assets and their supporting systems on a 'need-to-know' basis, including for remote access. Users shall be granted minimum access rights that are strictly required to execute their duties (principle of 'least privilege'), i.e. to prevent unjustified access to a large set of data or to prevent the allocation of combinations of access rights that may be used to circumvent controls (principle of 'segregation of duties').

b) User accountability: institutions shall limit, as much as possible, the use of generic and shared user accounts and ensure that users can be identified for the actions performed in the ICT systems.

c) Privileged access rights: institutions shall implement strong controls over privileged system access by strictly limiting and closely supervising accounts with elevated system access entitlements (e.g. administrator accounts). In order to ensure secure communication and reduce risk, remote administrative access to critical ICT systems shall be granted only on a need-to-know basis and when strong authentication solutions are used.

d) Logging of user activities: at a minimum, all activities by privileged users shall be logged and monitored. Access logs shall be secured to prevent unauthorised modification or deletion and retained for a period commensurate with the criticality of the identified business functions, supporting processes and information assets, in accordance with Section 3.3, without prejudice to the retention requirements set out in EU and national law. An institution shall use this information to facilitate the identification and investigation of anomalous activities that have been detected in the provision of services.

e) Access management: access rights shall be granted, withdrawn or modified in a timely manner, according to predefined approval workflows that involve the business owner of the information being accessed (information asset owner). In the case of termination of employment, access rights shall be promptly withdrawn.

f) Access recertification: access rights shall be periodically reviewed to ensure that users do not possess excessive privileges and that access rights are withdrawn when no longer required.

g) Authentication methods: institutions shall enforce authentication methods that are sufficiently robust to adequately and effectively ensure that access control policies and procedures are complied with. Authentication methods shall be commensurate with the criticality of ICT systems, information or the process being accessed. This shall, at a minimum, include complex passwords or stronger authentication methods (such as two-factor authentication), based on relevant risk.

36. Electronic access by applications to data and ICT systems shall be limited to a minimum required to provide the relevant service.

4.3 Physical security

37. Institutions' physical security measures shall be defined, documented and implemented to protect their premises, data centres and sensitive areas from unauthorised access and from environmental hazards.

38. Physical access to ICT systems shall be permitted to only authorised individuals. Authorisation shall be assigned in accordance with the individual's tasks and responsibilities and limited to individuals who are appropriately trained and monitored. Physical access shall be regularly reviewed to ensure that unnecessary access rights are promptly revoked when not required.

39. Adequate measures to protect from environmental hazards and malicious activities shall be commensurate with the importance of the buildings and the criticality of the operations or ICT systems located in these buildings.

4.4 ICT operations security

40. Institutions shall implement procedures to prevent the occurrence of security issues in ICT systems and ICT services and shall minimise their impact on ICT service delivery. These procedures shall include the following measures:

a) identification of potential vulnerabilities, which shall be evaluated and remediated by ensuring that software and firmware are up to date, including the software provided by institutions to their internal and external users, by deploying critical security patches or by implementing compensating controls;

b) implementation of secure configuration baselines of all network components;

c) implementation of network segmentation, data loss prevention systems and the encryption of network traffic (in accordance with the data classification);

d) implementation of protection of endpoints including servers, workstations and mobile devices; institutions shall evaluate whether endpoints meet the security standards defined by them before they are granted access to the corporate network;

e) ensuring that mechanisms are in place to verify the integrity of software, firmware and data; and

f) encryption of data at rest and in transit (in accordance with the data classification).

41. Furthermore, on an ongoing basis, institutions shall determine whether changes in the existing operational environment influence the existing security measures or require adoption of additional measures to mitigate related risks appropriately. These changes shall be part of the institutions' formal change management process, which shall ensure that changes are properly planned, tested, documented, authorised and deployed.

4.5 Security monitoring

42. Institutions shall establish and implement policies and procedures to detect anomalous activities that may impact institutions' information security and to respond to these events appropriately. As part of this continuous monitoring, institutions shall implement appropriate and effective capabilities for detecting and reporting physical or logical intrusion as well as breaches of confidentiality, integrity and availability of the information assets. The continuous monitoring and detection processes shall cover:

a) relevant internal and external factors, including business and ICT administrative functions;

b) transactions to detect misuse of access by third parties or other entities and internal misuse of access; and

c) potential internal and external threats.

43. Institutions shall establish and implement processes and organisation structures to identify and constantly monitor security threats that could materially affect their abilities to provide services. Institutions shall actively monitor technological developments to ensure that they are aware of security risks. Institutions shall implement detective measures, for instance to identify possible information leakages, malicious code and other security threats, and publicly known vulnerabilities in software and hardware, and shall check for corresponding new security updates.

44. The security monitoring process shall also help an institution to understand the nature of operational or security incidents, to identify trends and to support the organisation's investigations.

4.6 Information security reviews, assessment and testing

45. Institutions shall perform a variety of information security reviews, assessments and testing to ensure the effective identification of vulnerabilities in their ICT systems and ICT services. For instance, institutions may perform gap analysis against information security standards, compliance reviews, internal and external audits of the information systems, or physical security reviews. Furthermore, institutions shall consider good practices such as source code reviews, vulnerability assessments, penetration tests and red team exercises.

46. Institutions shall establish and implement an information security testing framework that validates the robustness and effectiveness of their information security measures and ensure that this framework considers threats and vulnerabilities, identified through threat monitoring and ICT and security risk assessment process.

47. The information security testing framework shall ensure that tests:

a) are carried out by independent testers with sufficient knowledge, skills and expertise in testing information security measures and who are not involved in the development of the information security measures; and

b) include vulnerability scans and penetration tests (including threat-led penetration testing where necessary and appropriate) commensurate to the level of risk identified with the business processes and systems.

48. Institutions shall perform ongoing and repeated tests of the security measures. For all critical ICT systems (para. 21), these tests shall be performed at least on an annual basis and, for PSPs, they shall be part of the comprehensive assessment of the security risks related to the payment services they provide, in accordance with Article 94(2) of Law 4537/2018. Non-critical systems shall be tested regularly using a risk-based approach, but at least every three (3) years.

49. Institutions shall ensure that tests of security measures are conducted in the event of changes to infrastructure, processes or procedures and if changes are made because of major operational or security incidents or due to the release of new or significantly changed internet-facing critical applications.

50. Institutions shall monitor and evaluate the results of the security tests and update their security measures accordingly without undue delays in the case of critical ICT systems.

51. For PSPs, the testing framework shall also encompass the security measures relevant to (1) payment terminals and devices used for the provision of payment services; (2) payment terminals and devices used for authenticating the payment service users (PSU); and (3) devices and software provided by the PSP to the PSU to generate/receive an authentication code.

52. Based on the security threats observed and the changes made, testing shall be performed to incorporate scenarios of relevant and known potential attacks.

4.7 Information security training and awareness

53. Institutions shall establish a training programme, including periodic security awareness programmes, for all staff and contractors to ensure that they are trained to perform their duties and responsibilities consistent with the relevant security policies and procedures to reduce human error, theft, fraud, misuse or loss and how to address information security-related risks. Institutions shall ensure that the training programme provides training for all staff members and contractors at least annually.

CHAPTER V. ICT OPERATIONS MANAGEMENT

54. Institutions shall manage their ICT operations based on documented and implemented processes and procedures (which, for PSPs, include the security policy document in accordance with Article 5(1)(j) of Law 4537/2018) that are approved by the Board of Directors. This set of documents shall define how institutions operate, monitor and control their ICT systems and services, including the documenting of critical ICT operations, and shall enable institutions to maintain up-to-date ICT asset inventory.

55. Institutions shall ensure that performance of their ICT operations is aligned to their business requirements. Institutions shall maintain and improve, when possible, efficiency of their ICT operations, including but not limited to the need to consider how to minimise potential errors arising from the execution of manual tasks.

56. Institutions shall implement logging and monitoring procedures for critical ICT operations to allow the detection, analysis and correction of errors.

57. Institutions shall maintain a complete and up-to-date inventory of their ICT assets (including ICT systems, network devices, databases, etc.). The ICT asset inventory shall store the configuration of the ICT assets and the links and interdependencies between the different ICT assets, to enable a proper configuration and change management process.

58. The ICT asset inventory shall be sufficiently detailed to enable the prompt identification of an ICT asset, its location, security classification and ownership. Interdependencies between assets shall be documented to help in the response to security and operational incidents, including cyber-attacks.

59. Institutions shall monitor and manage the life cycles of ICT assets, to ensure that they continue to meet and support business and risk management requirements. Institutions shall monitor whether their ICT assets are supported by their external or internal vendors and developers and whether all relevant patches and upgrades are applied based on documented processes. The risks stemming from outdated or unsupported ICT assets shall be assessed and mitigated.

60. Institutions shall implement performance and capacity planning and monitoring processes to prevent, detect and respond to important performance issues of ICT systems and ICT capacity shortages in a timely manner.

61. Institutions shall define and implement data and ICT systems backup and restoration procedures to ensure that they can be recovered as required. The scope and frequency of backups shall be set out in line with business recovery requirements and the criticality of the data and the ICT systems and evaluated according to the performed risk assessment. Testing of the backup and restoration procedures shall be undertaken on a periodic basis.

62. Institutions shall ensure that data and ICT system backups are stored securely and are sufficiently remote from the primary site so they are not exposed to the same risks.

5.1 ICT incident and problem management

63. Institutions shall establish and implement an incident and problem management process to monitor and log operational and security ICT incidents and

to enable institutions to continue or resume, in a timely manner, critical business functions and processes when disruptions occur. Institutions shall determine appropriate criteria and thresholds for classifying events as operational or security incidents, as well as early warning indicators that shall serve as alerts to enable early detection of these incidents. Such criteria and thresholds, for PSPs, are without prejudice to the classification of major incidents in accordance with Article 95 of Law 4537/2018 and ECA 157/3/2.4.2019.

64. To minimise the impact of adverse events and enable timely recovery, institutions shall establish appropriate processes and organisational structures to ensure a consistent and integrated monitoring, handling and follow-up of operational and security incidents and to make sure that the root causes are identified and eliminated to prevent the occurrence of repeated incidents. The incident and problem management process shall establish:

a) the procedures to identify, track, log, categorise and classify incidents according to a priority, based on business criticality;

b) the roles and responsibilities for different incident scenarios (e.g. errors, malfunctioning, cyber-attacks);

c) problem management procedures to identify, analyse and solve the root cause behind one or more incidents — an institution shall analyse operational or security incidents likely to affect the institution that have been identified or have occurred within and/or outside the organisation and shall consider key lessons learned from these analyses and update the security measures accordingly;

d) effective internal communication plans, including incident notification and escalation procedures — also covering security-related customer complaints — to ensure that:

i) incidents with a potentially high adverse impact on critical ICT systems and ICT services are reported to the relevant senior management and ICT senior management;

ii) the Board of Directors is informed on an ad hoc basis in the event of significant incidents and, at least, informed of the impact, the response and the additional controls to be defined as a result of the incidents;

e) incident response procedures to mitigate the impacts related to the incidents and to ensure that the service becomes operational and secure in a timely manner; and

f) specific external communication plans for critical business functions and processes in order to:

i) collaborate with relevant stakeholders to effectively respond to and recover from the incident; and

ii) provide timely information to external parties (e.g. customers, other market participants, the supervisory authority) as appropriate and in line with an applicable regulation.

CHAPTER VI. ICT PROJECT AND CHANGE MANAGEMENT

6.1 ICT project management

65. Institutions shall implement a programme and/or a project governance process that defines roles, responsibilities and accountabilities to effectively support the implementation of the ICT strategy.

66. Institutions shall appropriately monitor and mitigate risks deriving from their portfolio of ICT projects (programme management), considering also risks that may result from interdependencies between different projects and from dependencies of multiple projects on the same resources and/or expertise.

67. Institutions shall establish and implement an ICT project management policy that includes as a minimum:

a) project objectives;

b) roles and responsibilities;

c) a project risk assessment;

d) a project plan, timeframe and steps;

e) key milestones; and

f) change management requirements.

68. The ICT project management policy shall ensure that information security requirements are analysed and approved by a function that is independent from the development function.

69. Institutions shall ensure that all areas impacted by an ICT project are represented in the project team and that the project team has the knowledge required to ensure secure and successful project implementation.

70. The establishment and progress of ICT projects and their associated risks shall be reported to the Board of Directors, individually or in aggregation, depending on the importance and size of the ICT projects, regularly and on an ad hoc basis as appropriate. Institutions shall include project risk in their risk management framework.

6.2 ICT systems acquisition and development

71. Institutions shall develop and implement a process governing the acquisition, development and maintenance of ICT systems. This process shall be designed using a risk-based approach.

72. Institutions shall ensure that, before any acquisition or development of ICT systems takes place, the functional and non-functional requirements (including information security requirements) are clearly defined and approved by the relevant business management.

73. Institutions shall ensure that measures are in place to mitigate the risk of unintentional alteration or intentional manipulation of the ICT systems during development and implementation in the production environment.

74. Institutions shall have a methodology in place for testing and approval of ICT systems prior to their first use. This methodology shall consider the criticality of business processes and assets. The testing shall ensure that new ICT systems perform as intended. They shall also use test environments that adequately reflect the production environment.

75. Institutions shall test ICT systems, ICT services and information security measures to identify potential security weaknesses, violations and incidents.

76. Institutions shall implement separate ICT environments to ensure adequate segregation of duties and to mitigate the impact of unverified changes to production systems. Specifically, institutions shall ensure the segregation of production environments from development, testing and other non-production environments. Institutions shall ensure the integrity and confidentiality of production data in non-production environments. Access to production data shall be restricted to authorised users.

77. Institutions shall implement measures to protect the integrity of the source codes of ICT systems that are developed in-house. They shall also document the development, implementation, operation and/or configuration of the ICT systems comprehensively to reduce any unnecessary dependency on subject matter experts. The documentation of the ICT system shall contain, where applicable, at least user documentation, technical system documentation and operating procedures.

78. An institution’s processes for acquisition, development and decommissioning of ICT systems shall also apply to ICT systems developed or managed by the business function’s end users outside the ICT organisation (e.g. end user computing applications) using a risk-based approach. The institution shall maintain a register of these applications that support critical business functions or processes.

6.3 ICT change management

79. Institutions shall establish and implement an ICT change management process to ensure that all changes to ICT systems are recorded, tested, assessed, approved, implemented and verified in a controlled manner. Institutions shall handle the changes during emergencies (i.e. changes that must be introduced as soon as possible) following procedures that provide adequate safeguards.

80. Institutions shall determine whether changes in the existing operational environment influence the existing security measures or require the adoption of additional measures to mitigate the risks involved. These changes shall be in accordance with the institutions’ formal change management process.

CHAPTER VII. BUSINESS CONTINUITY MANAGEMENT

81. Institutions shall establish a sound business continuity management (BCM) process to maximise their abilities to provide services on an ongoing basis and to limit losses in the event of severe business disruption in line with Article 77(2) of Law 4261/2014 and Title VI of the EBA guidelines on internal governance (EBA/GL/2017/11).

7.1 Business impact analysis

82. As part of sound business continuity management, institutions shall conduct business impact analysis (BIA) by analysing their exposure to severe business disruptions and assessing their potential impacts (including on confidentiality, integrity and availability), quantitatively and qualitatively, using internal and/or external data (e.g. third party provider data relevant to a business process or publicly available data that may be relevant to the BIA) and scenario analysis. The BIA shall also consider the criticality of the identified and classified business functions, supporting processes, third parties and information assets, and their interdependencies, in accordance with Section 3.3.

83. Institutions shall ensure that their ICT systems and ICT services are designed and aligned with their BIA, for example with redundancy of certain critical components to prevent disruptions caused by events impacting those components.

7.2 Business continuity planning

84. Based on their BIAs, institutions shall establish plans to ensure business continuity (business continuity plans, BCPs), which shall be documented and approved by their Boards of Directors. The plans shall specifically consider risks that could adversely impact ICT systems and ICT services. The plans shall support objectives to protect and, if necessary, re-establish the confidentiality, integrity and availability of their business functions, supporting processes and information assets. Institutions shall coordinate with relevant internal and external stakeholders, as appropriate, during the establishment of these plans.

85. Institutions shall put BCPs in place to ensure that they can react appropriately to potential failure scenarios and that they are able to recover the operations of their critical business activities after disruptions within a recovery time objective (RTO, the maximum time within which a system or process must be restored after an incident) and a recovery point objective (RPO, the maximum time period during which it is acceptable for data to be lost in the event of an incident). In cases of severe business disruptions that trigger specific business continuity plans, institutions shall prioritise business continuity actions using a risk-based approach, which can be based on the risk assessments carried out under Section 3.3. For PSPs this may include, for

example, facilitating the further processing of critical transactions while remediation efforts continue.

86. An institution shall consider a range of different scenarios in its BCP, including extreme but plausible ones to which it might be exposed, including a cyber-attack scenario, and it shall assess the potential impact that such scenarios might have. Based on these scenarios, an institution shall describe how the continuity of ICT systems and services, as well as the institution's information security, are ensured.

7.3 Response and recovery plans

87. Based on the BIAs (para. 82) and plausible scenarios (para. 86), institutions shall develop response and recovery plans. These plans shall specify what conditions may prompt activation of the plans and what actions shall be taken to ensure the availability, continuity and recovery of, at least, institutions' critical ICT systems and ICT services. The response and recovery plans shall aim to meet the recovery objectives of institutions' operations.

88. The response and recovery plans shall consider both short-term and long-term recovery options. The plans shall:

a) focus on the recovery of the operations of critical business functions, supporting processes, information assets and their interdependencies to avoid adverse effects on the functioning of institutions and on the financial system, including on payment systems and on payment service users, and to ensure execution of pending payment transactions;

b) be documented and made available to the business and support units and readily accessible in the event of an emergency; and

c) be updated in line with lessons learned from incidents, tests, new risks identified and threats, and changed recovery objectives and priorities.

89. The plans shall also consider alternative options where recovery may not be feasible in the short term because of costs, risks, logistics or unforeseen circumstances.

90. Furthermore, as part of the response and recovery plans, an institution shall consider and implement continuity measures to mitigate failures of third party

providers, which are of key importance for an institution's ICT service continuity in line with the provisions of ECA 178/5/2.10.2020.

7.4 Testing of plans

91. Institutions shall test their BCPs periodically. In particular, they shall ensure that the BCPs of their critical business functions, supporting processes, information assets and their interdependencies (including those provided by third parties, where applicable) are tested at least annually, in accordance with para. 93.

92. BCPs shall be updated at least annually, based on testing results, current threat intelligence and lessons learned from previous events. Any changes in recovery objectives (including RTOs and RPOs) and/or changes in business functions, supporting processes and information assets, shall also be considered, where relevant, as a basis for updating the BCPs.

93. Institutions' testing of their BCPs shall demonstrate that they are able to sustain the viability of their businesses until critical operations are re-established. In particular they shall:

a) include testing of an adequate set of severe but plausible scenarios including those considered for the development of the BCPs (as well as testing of services provided by third parties, where applicable); this shall include the switch-over of critical business functions, supporting processes and information assets to the disaster recovery environment and demonstrating that they can be run in this way for a sufficiently representative period of time and that normal functioning can be restored afterwards;

b) be designed to challenge the assumptions on which BCPs rest, including governance arrangements and crisis communication plans; and

c) include procedures to verify the ability of their staff and contractors, ICT systems and ICT services to respond adequately to the scenarios defined in subparagraph (a) above.

94. Test results shall be documented by the officers in charge and validated by the internal audit function, and any identified deficiencies resulting from the tests shall be analysed, addressed and reported to the Board of Directors.

7.5 Crisis communications

95. In the event of a disruption or major security incident or emergency, and during the implementation of the BCPs, institutions shall ensure that they have effective crisis communication measures in place so that all relevant internal and external stakeholders, in particular:

a) the Bank of Greece;

b) the other competent authorities, when required by national regulations; and

c) relevant providers (group entities or third party providers),

are informed in a timely and appropriate manner.

CHAPTER VIII. PAYMENT SERVICE USER RELATIONSHIP MANAGEMENT

96. PSPs shall establish and implement processes to enhance PSUs' awareness of the security risks linked to the payment services by providing PSUs with assistance and guidance.

97. The assistance and guidance offered to PSUs shall be updated in the light of new threats and vulnerabilities, and changes shall be communicated to the PSU.

98. Where product functionality permits, PSPs shall allow PSUs to disable specific payment functionalities related to the payment services offered by the PSP to the PSU.

99. Where, in accordance with Article 68(1) of Law 4537/2018, a PSP has agreed with the payer spending limits for payment transactions executed through specific payment instruments, the PSP shall provide the payer with the option to adjust these limits up to the maximum agreed limit.

100. PSPs shall provide PSUs with the option to receive alerts on initiated and/or failed attempts to initiate payment transactions, enabling them to detect fraudulent or malicious use of their accounts.

101. PSPs shall keep PSUs informed about updates in security procedures that affect PSUs regarding the provision of payment services.

102. PSPs shall provide PSUs with assistance on all questions, requests for support and notifications of anomalies or issues regarding security matters related to

payment services. PSUs shall be appropriately informed about how such assistance can be obtained.

CHAPTER IX. FINAL PROVISIONS

103. This Act shall enter into force on the date of its publication in the Government Gazette.

104. As from the entry into force of this Act, the following shall be repealed:

(a) Annex 2 “Principles of secure and efficient operation of IT systems in the context of operational risk management by credit institutions” of Bank of Greece Governor's Act 2577/2006 “Framework of operational principles and criteria for the evaluation of the organisation and Internal Control Systems of credit and financial institutions and relevant powers of their management bodies” (Government Gazette A59);

(b) Executive Committee Act (“ECA”) 157/4/02.04.2019 “Adoption of the guidelines of the European Banking Authority on security measures for operational and security risks of payments services” (Government Gazette B1646), and any existing reference thereto shall be understood as a reference to this Act.

105. The Banking Supervision Department is hereby authorised to provide clarifications and guidance on the implementation hereof.

106. This Act shall be published in the Government Gazette and posted on the Bank of Greece website.

THE SECRETARY THE MEMBERS THE CHAIRMAN

Yannis Stournaras

True and exact copy,
Athens, 08.07.2021
The Secretary
(signed)
I. Pantou