NATIONAL BANK OF THE REPUBLIC OF MACEDONIA

Pursuant to Article 47 paragraph 1 item 6 of the Law on the National Bank of the Republic of Macedonia (Official Gazette of the Republic of Macedonia No. 158/10, 123/12, 43/14, 153/15, 6/16) and Article 68 paragraph 1 item 6 of the Banking Law (Official Gazette of the Republic of Macedonia No. 67/07, 90/09, 67/10, 26/13, 15/15, 153/15 and 190/16), and in connection with Article 48 paragraph 1 item 6 of the Law on the National Bank of the Republic of Macedonia, the National Bank of the Republic of Macedonia Council adopted the following

DECISION
on the Methodology for bank's information system security
(„Official Gazette of the Republic of Macedonia" No. 78/18)

I. GENERAL PROVISIONS

1. This Decision prescribes the Methodology for the bank's information system security which consists of rules for establishing process for managing the information system security, planning, development and implementation of the information technology management strategy, ensuring business continuity, as well as security rules regarding the electronic payment channels and the bank's outsourcing companies.

2. Security of the bank's information system, according to this Decision, means fulfillment of the following principles:

   - **Confidentiality**: the information system is accessible only to authorized users;
   - **Integrity**: protection of the accuracy and completeness of the information system;
   - **Availability**: unrestricted access to the information system for the authorized users.

II. DEFINITIONS

3. The terms used in this Decision have the following meaning:

3.1. “IT risk” is the risk of losses for the bank arising from lose, unauthorized usage, or unavailability of information, information assets and/or services that the bank provides.

3.2. "Information assets" represent the information regardless of the media where it is stored together with the software and the hardware components that provide access to the information, its processing, transmission and storage.

3.3. "Administrative security controls" include policies, standards, guidelines and procedures adopted by the bank’s management bodies, for establishing the process of information system security management.

3.4. "Technical security controls" represent the security measures integrated in the computer equipment, system software, communication equipment and the application programs.

3.5. "Physical security controls” are adequate measures for limiting and control of the physical access to the information assets in order to protect the bank from espionage, sabotage, fire, flood, vandalism, natural disasters and other types of damage or destruction of the entire, or part of the information system.

3.6. “Cybersecurity” is the ability of the bank to provide protection of the information assets and telecommunication networks from intrusions that may cause interruption, disabling, destruction or hostile takeover that may violate the information system security.

3.7. "Cybersecurity maturity level” represent the established practices, processes and behaviors in the bank that correspond to the certain level of the inherent risk, in order to support or increase the preparedness and resilience to the threats from cyberspace.

3.8. "Cybersecurity resilience" represents the ability of the bank to foresee, prepare and defend itself from cyber threats and to swiftly reestablish the functionality of the disrupted business processes.

3.9. "Major disruption of the business processes" represent a condition in which the bank is unable to meet its obligations due to the factors that are beyond its control, or a condition where the bank is physically damaged or there is damage to the telecommunications, i.e. when the information and the information systems for the critical operations are not available.

3.10. "Recovery Time Objective (RTO)" is the time period necessary for establishing the business processes with adequate technical support in the case of a major disruption of the business processes.

3.11. "Recovery Point Objective (RPO)" is the point in time that the data need to be recovered to and to continue with the business process in the case of a major disruption of the business processes.

3.12. "Electronic payment channel systems" are systems which offer banking services and products via interactive electronic communication channels by using the public telecommunication networks, such as remote access to the financial information, information regarding products and services, as well as systems for execution of the payment transactions.

3.13. "Payment transaction" is payment or transfer of funds, initiated by a payer or recipient, irrespective of the obligation between the payer and the recipient.

3.14. "Remote payment transaction " is a payment transaction initiated via Internet or by using the electronic device for remote communication.

3.15. "Transaction risk analysis" means evaluation of the risk related to a specific transaction taking into account the criteria such as the customer payment patterns (behavior), the value of the related transaction and the type of product and the payment recipient profile.

3.16. "Personalized security credentials" means personalized features provided by the bank for the purposes of user authentication when using the electronic payment channels.

3.17. "Major payment security incident" means an incident which has or may have a material impact on the security and continuity of the operation of the bank's payment systems or on the confidentiality of the payments and on the account balances. The assessment of materiality of the incident should consider the number of potentially affected customers, the amount and the impact on other payment systems and the overall infrastructure.

3.18. "User authentication" is a procedure that allows the bank to verify the identity of the users of the electronic payment channels, including the user's personalized security credentials.

3.19. "Monitoring of payment transactions" represent systems and mechanisms for monitoring and control of the transactions, fraud risk assessment and providing evidence for the transfer of certain information or that transactions are carried out by an authorized user.

3.20. "Sensitive payment data" represent payment transaction data, including the personalized security credentials, which may be used to carry out fraud.

3.21. "Outsourcing company" is:

- ancillary services company with prevailing activity of managing and maintaining data processing system and which processes and stores data for banking and financial activities, according to the written agreement; and/or
- an outsourcing provider, which according to a written agreement, processes and stores bank's data related to the banking and financial activities.

III. INFORMATION SYSTEM SECURITY MANAGEMENT PROCESS

4. For the purpose of achieving and continuous maintaining of the information system security, the bank is obliged to establish an information system security management process, which includes:
    - Risk assessment that includes the assessment of the information security risk as well the assessment of the cybersecurity risk;
    - Implementation of security controls;
    - Security testing and cybersecurity resilience testing
    - Monitoring and upgrading; and
    - Segregation of duties of the bank bodies related to the information system security management.

5. The information system security management process referred to in item 4 of this Decision is defined in the bank's Information System Security Policy, and should correspond to the nature, volume and the complexity of the financial activities and to the risks that the bank is exposed to during its operations.

Assessment of the information security risk and assessment of the cybersecurity risk

6. The assessment of the information security risk should include:
    - identification of the bank's information system assets;
    - classification of the bank's information system assets, i.e. assigning a value to the assets according to their importance;
    - analysis of the probability of threat occurrence in the information system by taking into account the harmful events, and the process of continuous analysis and monitoring of new weaknesses in the information system, especially taking into account the results of the performed tests referred to in the items 9 and 10 of this Decision;
    - prioritizing risks depending on the extent of the potential loss that they can cause.

    The bank is required to prepare a summary report at least annually for the assessment of the information system risks. The risks should be categorized according to the table given in the Annex 1 to this Decision.

7. The bank is required to establish a regular process for the assessment of the cybersecurity risk and to implement a strategy for achieving the cybersecurity maturity level. The process should include at least the following elements:
    - identifying factors that contribute to the increased level of cybersecurity risk;
    - determing the level of cybersecurity maturity level which corresponds with the identified cybersecurity risk;
    - proposing corrective measures that are required to raise its cybersecurity maturity level;
    - establishing process of information sharing with the other external institutions for the purpose of timely prevention of the cyber attacks.

The cybersecurity risk assessment should be performed in case of occurrence of new threats, in case of changes in the bank's business model by introducing new banking products and services, after significant changes in the organizational structure, after expanding into new markets, as well as after introducing new outsourcing companies and technology services providers.

Implementation of the security controls

8. The bank is obliged to adopt the Information System Security Policy under item 5 of this Decision which should include at least the following elements:
    - classification of both information and information assets according to their importance;
    - protection of personal data in accordance with the current local regulations;
    - methodology for risk assessment related to the information system security which defines the acceptable risk levels, and methodology for cybersecurity risk assessment and determining the level of the cybersecurity preparedness;
    - methods for ensuring cyberspace security and cyber resilience plan;
    - implementation of the bank's strategy for managing the identified risks and the cybersecurity maturity level, by establishing the action plan and budget for ensuring information system security;
    - annual plan for training of the persons with special rights and responsibilities, the bank's employees and clients, regarding the adequate use of services available via the bank's information system and informing about new cyber threats and frauds;
    - managing the various levels of security incidents and establishing adequate mechanism for their identification, reporting and efficient elimination by undertaking appropriate activities;
    - defining of the role of the IT organizational unit within the bank, which is obliged to have adequate human resources and internal working procedures, according to the adopted acts regarding the information system security;
    - defining adequate audit trail for the critical elements of the information system on several levels, such as operating system, data bases and telecommunication equipment, for the purpose of verifying the identity of the users and the order of the activities that are performed on the information system;
    - defining methods for security update management, upgrades to new versions, modification of the application parameters and source code changes, and preparation and new application releases;
    - defining the method for establishing the bank's Business Continuity Plan and adequate data protection;
    - methods for establishing anti-virus protection, protection against malicious programs and protection of the integrity of data;
    - defining the method for telecommunication interconnection and ensuring protection of the data that are being transferred;
    - defining the security zones in the bank, in order to restrict the physical access to the bank's information and the information assets;
    - defining the methods for establishing additional security mechanisms, such as fire prevention, flood protection, monitoring, sensors and alarms;
    - defining the role of the both internal and external audit for ensuring the security of the information systems; and
    - defining of the permitted exceptions to the Policy, the procedure for their approval and defining of the acceptable level of IT risk.

For the purpose of efficient implementation of the policy under this item, the bank is required to establish appropriate internal regulations.

The policy should contain description of the administrative, technical and physical security controls and the methods for their implementation.

Security testing and cybersecurity resilience testing

9. The bank is required to establish a process of professional, independent and objective testing of the efficiency and adequacy of the implemented security controls in the information system security policy.

10. The bank is obliged to conduct a professional and independent testing of its systems regarding cybersecurity resilience at least once every two years, according to the real-life scenarios and intelligence gathered, in order to verify the efficiency of the implemented controls and the adequacy of the cybersecurity maturity level.

    The volume, frequency and the scope of testing should be determined based on the level of the cybersecurity risk.

Monitoring and upgrading

11. The bank is obliged to establish a process for continuous collection and information analysis regarding the losses arising from the security incidents. The bank should establish an ongoing process for continuous collection and information analysis regarding the new weaknesses and threats to the information system, and to undertake activities to overcome them.

Segregation of duties of the bank's management bodies with respect to the information system security management

12. The bank should establish adequate organizational structure for information system security management, with clearly defined competencies and responsibilities of the bank's management bodies in the information system security management process.

    The Supervisory Board is responsible for adopting the information system security policy and monitoring its implementation on an annual basis.

    The Risk Management Committee is responsible for establishing an information system security policy, monitoring its implementation, analyzing the reports on the exposure to IT risk, and for proposing strategies, measures and risk mitigation instruments.

    The Management Board should create an information system security policy and is responsible for managing and monitoring the IT risk that the bank is exposed to.

13. For the purpose of managing the information system security, the Bank should appoint an Information System Security Officer who is responsible for coordination of the information system security policy and the processes related to various technological platforms and tasks.

The person under paragraph 1 of this item should be independent from the persons employed in the bank's organizational units that undertake risks related to the information systems security.

The Information System Security Officer should produce reports for the Supervisory Board regarding the activities related to the information system security, at least biannually.

14. The reporting under item 13 paragraph 3 of this Decision should contain at least the following elements:
    - information regarding the identified risks and their control;
    - permitted exceptions to the Information System Security Policy in accordance with item 8 paragraph 1 indent 17 of this Decision, by indicating the associated risks;
    - information regarding the agreements with the outsourcing companies;
    - results of the information system security testing, security incidents and appropriate activities by the bank management bodies; and
    - requests for changes in the bank's information system security policy, for the purpose of its improvement.

IV. PLANNING, DEVELOPMENT AND IMPLEMENTATION OF THE IT MANAGEMENT STRATEGY

15. The bank is required to establish a framework for planning and developing of the adequate IT management strategy (hereinafter: IT strategy) proportionate to the nature, volume and the complexity of its IT activities.

16. The bank is required to adopt, document and support the IT strategy by developing operational plans for achieving realistic goals, by appropriate resource planning and budgeting within defined time periods.

    The IT strategy should be in compliance with the bank's business policy. It should be periodically updated, particularly when the business model is being changed, in order to ensure continued alignment of the IT and business plans and activities.

17. The bank is required to establish a control framework appropriate to its size, IT activities, the level of change activities as well as changes with material implications for the institution's business model, to support the effective implementation of the institution's IT strategy by implementing an adequate project organization, budget monitoring and regular reporting.

18. The bank is required to define roles and responsibilities for the bank's management bodies as well as for other relevant bodies regarding the implementation of the IT strategy, that have relevant experience in organization and oversight of the major and complex technology changes.

19. The bank is required to identify and assess the risks associated with successful implementation of the IT strategy, as well as to undertake measures for their mitigation.

V. ENSURING BUSINESS CONTINUITY

20. The bank is required to develop and implement its own business continuity plan based on several scenarios and which will ensure its functionality and will mitigate the losses in a case of major disruption of the business processes.

21. The plan under item 20 of this Decision should identify the bank's critical operations, including those relying on the outsourcing companies, or third parties. For these processes, the bank should:
    - develop the methodology for Business Impact Assessment (BIA) and define the parameters for the Maximum Tolerable Downtime (MTD) for critical business lines and define the parameters for Recovery Time Objective (RTO) and Recovery Point Objective (RPO);
    - identify the alternative mechanisms for continuation of business processes in case of disruption of the primary mechanisms;
    - identify the methods for data backup and recovery, necessary for the business process continuity at a remote location;
    - choose the Disaster Recovery Location (DRL) where the data will be protected and which should be located at an adequate geographical distance from the primary location, in order to minimize the risk of simultaneous unavailability of both locations;
    - take into consideration the possible solutions to overcome the risks to the continuity and availability of IT systems and services that may arise from cyber attacks and to prepare an appropriate cybersecurity resilience plan;
    - take into consideration the physical measures for protection of the bank’s critical infrastructure at the both primary and disaster recovery location and to provide appropriate conditions for their smooth and safe operation;
    - take into consideration the roles and responsibilities of the persons responsible for the IT infrastructure when outsourced services are being used, by preparing adequate plans and activities for ensuring continuity and resilience in the operations.

    For efficient implementation of the plan under item 20 of this Decision, the bank is required to establish procedures for adequate implementation of the elements defined under paragraph 1 of this item.

    The bank is obliged to provide IT systems for the disaster recovery location with adequate capacity and availability in accordance with the parameters referred to in paragraph 1 indent 1 of this item, in order to provide conditions for smooth operation of the designated personnel in crisis conditions.

22. The bank is obliged to perform annual testing of the business continuity by developing complex scenarios and involving larger number of systems and participants.

    The scenarios should include at least testing of the following systems: core banking application, interconnection with the payment systems in the country and abroad (NBRM, KIBS, SWIFT).

    The bank is required to submit to the National Bank the summary report on the results of the performed tests.

23. Depending on the size, the nature and the volume of the financial activities of the Bank, the Governor of the National Bank has right to define the parameters for the

recovery time objective and the recovery point objective for the business processes defined in item 21 paragraph 1 of this Decision.

VI. ELECTRONIC PAYMENT CHANNEL SYSTEMS

24. Along with the criteria referred to in item 2 of this Decision for the electronic payment channel systems that provide remote access to the bank with options for executing remote payment transactions, the information system security should ensure user authentication and monitoring of payment transactions.

User authentication

25. User authentication can be performed via three elements: knowledge (something only the user knows), possession (something only the user posses) and/or inherence (something the user is). These elements are implemented by using the following methods:
    - knowledge: through set of symbols known only by the user, such as password, PIN;
    - possession: through device owned by the user only, such as mobile phone, electronic card, key (token), digital certificate, one-time authorization code and/or
    - inherence: through some of the unique biometric characteristics of the user, such as fingerprint, iris, voice or face recognition, palm geometry.

    The elements referred to in paragraph 1 of this item should be mutually independent, i.e. the breach of one does not compromise the reliability of the others. At least one of the elements should be non-reusable and non-replicable, and not capable of being surreptitiously stolen via the Internet.
26. The bank should implement secure and efficient methods for user authentication and authorization for electronic payment channel systems.

27. For the electronic payment channel systems that are available via the Internet, the bank is required to provide valid confirmation of its identity through the communication channel, so that users can verify the identity of the bank's system.

28. The bank should provide secure methods for customer enrolment and initial provision of the authentication tools as well as to ensure the integrity of the payment-related software.

29. All the data used for user identification, authentication and authorization for the electronic payment channel systems should be appropriately secured against theft and unauthorized access or modification.

30. For the electronic payment channel systems that include execution of payment transactions, payment cards data, changes in customer’s personal data, changes in the authorized lists of payment recipients (so-called white lists), the Bank should implement methods for strong customer authentication, by combining at least two of the elements defined in item 25 of this Decision.

As an exception to paragraph 1 of this item, the strong customer authentication for payment transactions via electronic payment channel systems is not mandatory in the following cases:

- internal transfers between two accounts of the same client;
- internal transfers in the Bank, justified by a transaction risk analysis, and
- individual payment transactions with low value, justified by a transaction risk analysis.

Monitoring of payment transactions

31. The electronic payment channels should provide mechanisms for monitoring the client's activities and payment transactions in order to provide prevention, detection and additional screening for potential fraud. These mechanisms should be activated before any final authorization of payments.

    The mechanisms referred to in paragraph 1 of this item shall be based at least on the following parameters/rules and/or indicators:

    - introducing a so-called black lists containing compromised clients' data and stolen cards data, black lists of IBAN numbers, data on forged documents of clients;
    - abnormal behavior of the client or unusual change of the access to the electronic payment channels (e.g. change of the Internet Protocol (IP) addresses of the client or change of the IP range (geolocation) during one or more sessions, so-called impossible travel, atypical payments to a certain e-merchant categories for a specific customer, abnormal transaction data).

32. The bank should implement systems that are able to detect signs of malicious software in the established remote channel (session) and are able to detect known fraud scenarios. The extent, complexity and adaptability of these systems should be commensurate with the outcome of the risk assessment.

33. The procedure for control and evaluation of frauds related to high-risk payment transactions should be carried out in an appropriately defined time period, in order not to unduly delay the execution of payments.

34. If the bank decides, in accordance with its risk analysis and assessment, to perform an additional verification of the payment transaction which has been identified as potentially fraudulent, it should be carried out within appropriately defined time period, or until the criteria referred to in item 24 of this Decision are met.

35. The bank should implement adequate audit trails in the electronic payment channel systems to verify the order of the activities being performed.

36. Banks should provide assistance and guidance to customers on the adequate use of the electronic payment channel systems and their new features, as well as on secure payment execution.

    Banks should inform their customers at least of the following procedures:

    - protection of their passwords, mobile devices, security keys (tokens) and devices for verification of the transactions executed via electronic payment channels;
    - adequate and secure use of the client's personal devices such as personal computer, mobile phone and updating of the user's security components such as: anti-virus, firewall, security patches, etc.;

- use of the genuine internet address of the bank which is used for executing payment transactions and for download of the payment-related software;
- methods for submitting user's complaints, providing user support, reporting of suspicious and/or altered transactions, abnormal software behavior, anomalies during the use of the electronic payment channel services, and/or possible social engineering attempts;
- the bank's response regarding the submitted complaints of potential frauds, and/or warnings to the user for occurrence of potential attacks or threats in the electronic payment channel system;

If the bank communicates with its users electronically, it should provide a way for validation of the authenticity of the messages that it sends to the clients.

37. The bank should define and set limits on the payments executed via electronic payment channels and provide its users with options for further limitation within these limits. Limits on payments may apply to all of the payments carried out via the electronic payment channel or for a specific remote communication channel and/or banking product and service.

    The bank should at least establish the following limits:
    - maximum amount for each individual payment made through electronic payment channels, and
    - cumulative amount of payments over a certain period of time (day, month).

    The bank should inform its users for the established limits referred to in paragraph 1 of this item.

38. Electronic statements exchanged with the users should be available in a trusted and safe environment. If the bank periodically informs its clients by delivering regular electronic reports, or ad-hoc (after initiated/executed payment transactions) through alternative channel, the sensitive payment data should be masked or not be included at all.

VII. OUTSOURCING COMPANY

39. The outsourcing company is obliged to be certified in accordance with the international standard ISO/IEC 20000.

40. The bank intending to conclude an agreement with an outsourcing company should meet at least the following criteria:

    40.1. To provide data backup from its databases regarding the operations over the last three years. The data backup should be kept on the locations stated in sub-item 40.2. and sub-item 40.3. of this item. The bank should perform regular updates of the data backups, according to the Policy under item 8 of this Decision, and at least once in every 24 hours;

    40.2. To possess at least one functional information system located on the territory of the Republic of Macedonia, which will include at least the following sub-systems:
    - retail banking operations and legal entities,

- accounting operations,
- domestic and foreign payment operations; and
- other sub-systems, which according to the item 21 of this Decision are assessed as critical operations for the business continuity;

40.3. To possess additional autonomous information system, located in the Republic of Macedonia if the company under paragraph 1 of this item is located abroad. The additional autonomous information system should be at an adequate distance from the system referred to in sub-item 40.2. of this paragraph. The additional information system should possess adequate reporting subsystems for preparing up-to-date reports for the bank management bodies, reports for the National Bank, as well as reports for other bodies or institutions in accordance with the regulations in the Republic of Macedonia.

In the bank intends to use outsourcing services for payment card processing, the criteria in this item should not apply.

41. Before the outsourcing company is selected, the bank should undertake the following activities:
    - to perform due diligence of the company's operations from legal and financial aspect; and
    - to perform assessment of the risks on the bank's operations that may arise from the use of the outsourced services in the area of the information system, while processing banking and financial activities.

    The selection of the outsourcing company means conclusion of new agreement or renewing the current one.

42. The bank should not conclude agreement with the outsourcing company, if the agreement in any way, prevents, restricts or obstructs National Bank's access while performing supervision or oversight, in conformity with the Banking Law.

43. The outsourcing company must not use services provided by other outsourcing companies, i.e. subcontractors, for processing of the services agreed in the contract, unless it is explicitly stated.

44. The operations of the outsourcing company should be harmonized with the bank’s policy under item 8 of this Decision.

45. The bank which made a decision to use outsourced services, besides the elements in the policy defined in item 8 paragraph 1 of this Decision, should also include the following policy elements:
    - defining the methods for determining the principles and rules for company selection;
    - defining the protection mechanisms that should be included in the contract, such as: clause for non-disclosure of information, clause for the level of the quality of services, clause for coordinated management of security incidents, clause for conducting independent audit, etc.;
    - determining standards the company should meet and which should be harmonized with the bank's business continuity plan and the cybersecurity resilience plan;

- defining the methods of monitoring the quality of services, company's operations, financial condition and its risk profile, through periodical testing of its compliance with the bank's information system security policy and its cybersecurity maturity level.

46. When the bank uses outsourcing company for providing SWIFT services for the bank's international payment operations, it should:

- organize the SWIFT service functions according to the items 41, 42, 44 and 45 of this Decision;
- provide a set of standardized software tools for adequate management of message exchange;
- appoint at least two full-time employees responsible for the security of the SWIFT infrastructure (SWIFTNet Security Officers). These employees should have unrestricted online and offline access to the services for the management of the SWIFT's certificate infrastructure (SWIFTNet PKI);
- appoint an additional SWIFTNet Security Officer, if needed, who does not need to be a full-time employee. In such case, the activities of SWIFTNet Security Officers have to be implemented on the principle of dual authorization;
- not implement the principle of shared security officers for the certificate infrastructure management, if this approach prevents the unrestricted access of the persons referred to in paragraph 1, indent 3 of this item.

VIII. REPORTING

47. The bank is required to inform the National Bank whenever it identifies the highest level of security incident in the information system and a major incident related to the payment security, according to the defined levels of security incidents under item 8 paragraph 1 indent 7 of this Decision.

    The bank is required to send the notification under paragraph 1 of this item to the National Bank, no longer than three days from the day it is determined that security incident occurred.

48. The bank is required to send the summary report on the identified risks for the information system, referred to in item 6 paragraph 2 of this Decision, by the end of the current year.

49. The bank is required to notify the National Bank on the changes in the key parts of the process for the information system security management, particularly in the case of changes in the elements of the policy defined in item 8 paragraph 1 of this Decision.

IX. TRANSITIONAL AND CLOSING PROVISIONS

50. This Decision shall enter into force on the eighth day after the date of its publication in the Official Gazette of the Republic of Macedonia, and shall apply from 1 January 2019.

The bank is required to comply with item 31 and item 32 of this Decision as of 1 January 2020.

51. With the implementation of this Decision, the Decision on the bank's information system security (Official Gazette of the Republic of Macedonia, No. 31/2008, 78/08, 31/09 and 74/12) shall cease to be effective.

D. No. 02-15/VIII-1/2018
26 April 2018
Skopje

Governor
and Chairman
of the Council of the National Bank
of the Republic of Macedonia

Dimitar Bogov

Annex 1 - IT risk categorization (recommendations for unification of the IT risk categories in the EU[1])

IT RISK CATEGORY	DEFINITION
I. Risk to the continuity and availability of IT systems	Risk of events that may adversely affect the operation and availability of IT systems and data, including the inability to timely establish the services of the institution due to malfunctions in the hardware and software components of IT systems, weaknesses in the management of IT systems or other events.
II. Risk to IT security	Risk arising from unauthorized access to IT systems and data from inside the Bank and outside the Bank (e.g. intrusions from the digital space).
III. Risk of changes in IT	Risk arising from the Bank's inability to manage the changes in IT systems in a timely and controlled manner, especially when it comes down to major and complex changes in the applications.
IV. Risk to the integrity of IT data	Risk that data stored and processed on IT systems is incomplete, inaccurate or inconsistent in different IT systems, for example due to weak or non-existent controls over the life cycle of the data (designing the data topology, developing the data model and/or data dictionary, verification of the data entry, control over the data extraction, transmission and processing, including also output data), thereby disturbing the Bank's ability to rightly and timely provide services and information related to the (risk) management with the Bank.
V. Risks associated with the use of the outsourcing companies	Risk arising from the engagement of the Company or part of a group to maintain an IT system in which bank data is stored and bank and financial activities are processed, whereby such manner of work adversely affects the Bank's operations and the manner of its risk management.

The definitions of all IT risk categories also include examples of IT risks with their description which are stated in the following table attached to this Annex 1.

Annex: IT risk categories and a certain number of IT risks that have great potential and may cause operational interruptions with material and financial damage and/or damage the Bank's reputation

[1] Guidelines on ICT Risk Assessment under the SREP (European Banking Authority - EBA/GL/2017/05)

Categories of IT risk	IT risk (the list is not comprehensive[2])	Risk description	Examples
ICT availability and continuity risks	*Inadequate capacity management*	A lack of resources (e.g. hardware, software, staff, service providers) can result in an inability to scale the service to meet business needs, system interruptions, degradation of service and/or operational mistakes.	- A capacity shortfall may affect transmission rates and the availability of the network (internet) for services like internet banking. - A lack of staff (internal or third party) can result in system interruptions and/or operational mistakes.
	ICT system failures	A loss of availability due to hardware failures.	- Failure/malfunction of storage (hard disks), server or other ICT equipment caused by e.g. lack of maintenance.
		A loss of availability due to software failures and bugs.	- Infinite loop in application software prevents transaction execution. - Outages due the continued use of outdated ICT systems and solutions that no longer meet present availability and resilience requirements and/or are no longer supported by their vendors.
	Inadequate ICT continuity and disaster recovery planning	Failure of ICT planned availability and/or continuity solutions and/or disaster recovery (e.g. fall-back recovery datacenter) when activated in response to an incident.	- Configuration differences between the primary and secondary datacenter may result in the incapacity of the fall-back datacenter to provide the planned continuity of service.

[2] ICT risks are listed under the risk category they most impact but they may impact other risk categories.

	Disruptive and destructive cyber attacks	Attacks for different purposes (e.g. activism, blackmailing), which result in an overloading of systems and the network, preventing online computer services to be accessed by their legitimate users.	• Distributed Denial of Service attacks are performed by means of a multitude of computer systems on the internet controlled by a hacker, sending a large amount of apparently legitimate service requests to internet (e.g. e-banking) services.
ICT security risks	*Cyber-attacks and other external ICT based attacks*	Attacks performed from the internet or outside networks for different purposes (e.g. fraud, espionage, activism / sabotage, cyber terrorism) using a variety of techniques (e.g. social engineering, intrusion attempts through the exploitation of vulnerabilities, deployment of malicious software) resulting in taking control of internal ICT systems.	Different types of attacks: • APT (Advanced Persistent Threat) for taking control of internal systems or stealing information (e.g. identity theft related information, credit card information). • Malicious software (e.g. ransomware) that encrypts data with the aim of blackmail. • Infection of internal ICT systems with Trojan horses for committing malicious system actions in a hidden manner. • Exploitation of ICT system and/or (web) application vulnerabilities (e.g. SQL injection …) to gain access to the internal ICT system.
		Execution of fraudulent payment transactions by hackers through the breaking or circumvention of the security of e-banking and payment services and/or by attacking and exploiting security vulnerabilities in the internal payment systems of the institution.	• Attacks against e-banking or payment services, with objective to commit unauthorised transactions. • The creation and sending out of fraudulent payment transactions from within the internal payment systems of the institution (e.g. fraudulent SWIFT messages).

		Execution of fraudulent securities transactions by hackers through the breaking or circumvention of the security of the e-banking services that also provide access to the customer's securities accounts.	• Pump and dump attacks where the attackers gain access to e-banking securities accounts of customers and place fraudulent buying or selling orders to influence the market price and /or make gains based on previously established securities positions.
		Attacks on communication connections and conversations of all kinds or ICT systems with the objective of collecting information and/or committing frauds.	• Eavesdropping/intercepting unprotected transmission of authentication data in plain-text.
	Inadequate internal ICT	Gaining unauthorised access to critical ICT systems from within the institution for different purposes (e.g. fraud, performing and hiding rogue trading activities, data theft, activism / sabotage) by a variety of techniques (e.g. abusing and/or escalating privileges, identity theft, social engineering, exploiting vulnerabilities in ICT systems, deployment of malicious software).	• Installing key stroke loggers (key loggers) to steal user IDs and passwords to gain unauthorised access to confidential data and/or commit fraud. • Cracking/guessing weak passwords to gain illegitimate or elevated access rights. • System administrator uses operating systems or database utilities (for direct database modifications) to commit fraud.
		Unauthorised ICT manipulations due to inadequate ICT access management procedures and practices.	• Failure to disable or delete unnecessary accounts such as those of staff that changed functions and/or left the institution, including guests or suppliers who no longer need access, providing unauthorised access to ICT systems. • Granting excessive access rights and privileges, allowing unauthorised accesses and/or making it possible to hide rogue

			activities.
		Security threats due to lack of security awareness whereby employees do not understand, neglect or fail to adhere to ICT security policies and procedures.	• Employees that are deceived into providing assistance for an attack (i.e. social engineering). • Bad practices regarding credentials: sharing passwords, using ‘easy’ to guess passwords, using the same password for many different purposes, etc. • Storage of unencrypted confidential data on laptops and potable data storage solutions (e.g. USB keys) that can be lost or stolen.
		The unauthorised storage or transfer of confidential information outside the institution.	• Persons stealing or deliberately leaking or smuggling out confidential information to unauthorised persons or the public.
	Inadequate physical ICT security	Misuse or theft of ICT assets via physical access causing damage, loss of assets or data or to make other threats possible.	• Physically breaking into office buildings and/or data centers to steal ICT equipment (e.g. computers, laptops, storage solutions) and/or to copy data by physically accessing ICT systems.
		Deliberate or accidental damage to physical ICT assets caused by terrorism, accidents or unfortunate/erroneous manipulations by staff of the institution and/or third parties (suppliers, repairman).	• Physical terrorism (i.e. terrorist bombs) or sabotage of ICT assets. • Destruction of data center caused by fire, water leakage or other factors.

		Insufficient physical protection against natural disasters resulting in partial or complete destruction of ICT systems/datacenters by natural disasters.	• Earthquakes, extreme heat, wind storms, heavy snowstorms, floods, fire, lightning.
ICT change risks	*Inadequate controls over ICT system changes and ICT development*	Incidents caused by undetected errors or vulnerabilities as a result of change (e.g. Unforeseen effects of a change or a poorly managed change due to a lack of testing or improper change management practices) to e.g. software, ICT systems and data.	• Release into production of insufficiently tested software or configuration changes with unexpected adverse effects on data (e.g. corruption, deletion) and/or ICT system performance (e.g. breakdown, performance degradation). • Uncontrolled changes to ICT systems or data in the production environment. • Release into production of ill-secured ICT systems and internet applications, creating opportunities for hackers to attack the provided internet services and /or to breach the internal ICT systems. • Uncontrolled changes in the source code of internally developed software. • Insufficient testing due to the absence of adequate testing environments.
	Inadequate ICT architecture	A weak ICT architecture management when designing, building and maintaining ICT systems (e.g. software, hardware, data) can lead, over time, to complex, difficult, costly to manage and rigid ICT systems, that are no longer sufficiently aligned with business needs and are falling short compared to actual risk management requirements.	• Inadequately managed changes to ICT systems, software and/or data over a prolonged period of time, leading to complex, heterogeneous and difficult to manage ICT systems and architectures, causing many adverse business and risk management impacts (e.g. lacking flexibility and agility, ICT incidents and failures, high operating cost, weakened ICT security and resiliency, reduced data quality and reporting capabilities).

			• Excessive customisation and extension of commercial software packages with internally developed software, leading to the incapacity to implement future releases and upgrades of the commercial software and the risk of no longer being supported by the vendor.
	Inadequate lifecycle and patch management	The failure to maintain an adequate inventory of all ICT assets in support of, and in combination with, sound life-cycle and patch management practices. This leads to insufficiently patched (and thus more vulnerable) and outdated ICT systems that may not support business and risk management needs.	• Unpatched and outdated ICT systems that may cause adverse business and risk management impacts (e.g. lacking flexibility and agility, ICT outages, weakened ICT security and resilience).
ICT data integrity risks	*Dysfunctional ICT data processing or handling*	Due to system, communication and/or application errors or failures, or erroneously executed data extraction, transfer and load (ETL) process, data could be corrupted or lost.	• IT system error in batch processing, causing incorrect balances in client's bank accounts. • Wrongly executed queries. • Data loss due to data replication (backup) error.
	Ill designed data validation controls in ICT systems	Errors relating to missing or ineffective automated data input and acceptance controls (e.g. for used third party data), data transfer, processing and output controls in the ICT systems (e.g. input validity controls, data reconciliations).	• Insufficient or invalid formatting/validation of data inputs in applications and/or user interfaces. • Absence of data reconciliation controls on produced outputs • Absence of controls on the executed data extraction processes (e.g. database queries) leading to erroneous data. • Use of faulty external data.
	Ill controlled data changes in the	Data errors introduced due to lack of controls on the correctness and justified nature of data manipulations performed in the production of	• Developers or database administrators directly accessing and changing the data in

	production ICT systems.	ICT systems	the production ICT systems in a non-controlled way e.g. in the case of an ICT incident.
	Ill designed and/or managed data architecture, data flows, data models or data dictionaries	Ill managed data architectures, data models, data flows or data dictionaries may result in multiple versions of the same data across the ICT systems, which are no longer consistent due to differently applied data models or data definitions, and/or differences in the underlying data generation and change process.	• The existence of different customer databases per product or business unit with different data definitions and fields, resulting in unreconciled and difficult to compare an integrate customer data at the level of the whole financial institution or group.
ICT outsourcing risks	*Inadequate resilience of third party or another Group entity services*	The non-availability of critical outsourced ICT services, telecommunication services and utilities. Loss or corruption of critical/sensitive data entrusted to the service provider	• Unavailability of core services as a result of failures in suppliers (outsourced) ICT systems or applications. • Disruption of telecommunication links. • Power supply shortage.
	Inadequate outsourcing governance	Major service degradation or failures due to inefficient preparedness or control processes of the outsourced service provider. Ineffective outsourcing governance may result in a lack of appropriate skills and capabilities to fully identify, assess, mitigate and monitor the ICT risks and can limit institutions' operational capabilities.	• Poor incident handling procedures, contractual control mechanisms and guarantees built into the service provider agreement that increase key man dependency on third parties and vendors. • Inappropriate change management controls concerning the service provider ICT environment can cause major service degradation or failure.

	Inadequate security of third party or another Group entity	Hacking of the third party service providers' ICT systems, with a direct impact on the outsourced services or critical/confidential data stored at the service provider. Service provider staff gaining unauthorised access to critical/sensitive data stored at the service provider	• Hacking of service providers by criminals or terrorists, as an entry point into the institutions' ICT systems or to access /destroy critical or sensitive data stored at the service provider. • Malicious insiders at the side of the service provider try to steal and sell sensitive data.