Final text

Decision on adequate information system management

September 2022

Pursuant to Article 101, paragraph (2), item (1) of the Credit Institutions Act (Official Gazette 159/2013, 19/2015, 102/2015, 15/2018, 70/2019, 47/2020 and 146/2020) and Article 43, paragraph (2), item (10) of the Act on the Croatian National Bank (Official Gazette 75/2008, 54/2013 and 47/2020), the Governor of the Croatian National Bank hereby issues the

Decision on adequate information system management

I GENERAL PROVISIONS

Subject matter
Article 1

This Decision prescribes in detail the obligations of a credit institution relating to information system management and the information and communication technology risk management.

Entities subject to the Decision
Article 2

(1) The provisions of this Decision shall apply to a credit institution which has its registered office in the Republic of Croatia and which is authorised by the Croatian National Bank.
(2) The provisions of this Decision shall apply, mutatis mutandis, to the branche of a third-country credit institution authorised by the Croatian National Bank to establish a branch of a third-country credit institution.

Definition of terms
Article 3

(1) For the purposes of this Decision, the following terms shall have the following meaning:
1) '*information and communication technology*' (hereinafter referred to as '*ICT')* means the technology that ensures automated collection, processing, generating, storage, transmission, presentation and distribution of information, and the disposal thereof;
2) '*information system*' *(*hereinafter referred to as '*ICT system')* means the information and communication technology, which is regulated as part of the mechanism or an interconnected network providing support to the operations of a credit institution;
3) '*information asset*' means a collection of information, either tangible or intangible, that is worth protecting;
4) '*ICT asset*' means a software or hardware asset that is found in the business environment;
5) '*ICT services*' means services provided by ICT systems to users; examples include data entry, data storage and data processing and reporting services, but also monitoring, and business and decision support services;
6) '*ICT project*' means any project, where ICT systems and services are changed, replaced, dismissed or implemented; ICT projects can be part of wider ICT programmes or business transformation programmes;
7) '*ICT system users*' means any persons using the ICT system (a credit institution's employees, service providers, a credit institution's clients, etc.);

8) '*confidentiality*' means a property of information (data) that is not made available or may not be disclosed to unauthorised entities;
9) '*integrity*' means a property of information (data) and processes implying that it has not been subject to unauthorised or unforeseen alterations;
10) '*availability*' means a property of information and processes implying that these information and processes are accessible and usable, i.e. timely available to an authorised user at his/her request;
11) '*authenticity*' means a property implying that a party's identity is as claimed;
12) '*information security*' means the preservation of confidentiality, integrity and availability of information and the ICT system; for the purposes of this Decision, information security refers to the information contained in the ICT system;
13) '*operational or security incident*' (hereinafter referred to as '*ICT incident*') means a singular event or a series of linked events unplanned by the credit institution that has or will probably have an adverse impact on the integrity, availability, confidentiality and/or authenticity of ICT services;
14) '*cyber-attack*' means a malicious activity aimed at threatening information security, which may result in an ICT-related incident;
15) '*log*' means a note on the activities on ICT assets generated in the chronological order as these activities were performed (operation system log, firewall log, router log, intrusion detection system and activities on the ICT system log, application software log, database log, etc.);
16) '*ICT risk*' means 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 ICT within a reasonable time and with reasonable costs when the environment or business requirements change (i.e. agility); ICT risk includes security risks arising out of inadequate or failed internal processes or external events including cyber-attacks or inadequate physical security;
17) '*information security testing*' means the verification of reliability and efficiency of information security controls;
18) '*information security reviews, assessment and testing*' means the procedures that can include the gap analyses against information security standards, compliance reviews, internal and external audits of the ICT systems, physical security reviews, source code reviews, vulnerability assessments, penetration tests (including threat-led penetration testing) and red team exercises;
19) '*administrative controls*' include the adoption of internal bylaws relating to the ICT system and setting up of an appropriate organisational structure and the implementation of internal bylaws relating to the ICT system, with a view to ensuring its functionality and safety;
20) '*logical controls*' means the controls implemented in the software components of an information system;
21) '*physical controls*' means the controls protecting the ICT system from unauthorised physical access, theft, physical damage or destruction;
22) '*third party*' means a natural or legal person that has entered into a business relationship or contract with a credit institution to provide a product or service, including outsourcing service providers;
23) '*business impact analysis*' means the procedure of the assessment of activities (business processes) and impacts business disruptions may have on them;
24) '*recovery time objective*' means an acceptable period of unavailability of a credit institution's business processes and information system resources necessary for their carrying out, i.e. the time required to restore (recover) the business processes;
25) '*recovery point objective*' means the maximum time period during which it is acceptable for data to be lost in the event of an incident.

(2) The other terms used in this Decision shall have the meaning in accordance with Article 3 of the Credit Institutions Act.

II GOVERNANCE AND ICT STRATEGY

Governance
Article 4

(1) A credit institution's management board shall:
1) have adequate ICT risk governance and control framework in place;
2) set clear roles and responsibilities within the credit institution, including those for the management board and its committees; and
3) have in place adequate functions with regard to the management of the information and communication technology, ICT risk, ICT system security and business continuity.
(2) A credit institution's management board shall be accountable for setting, approving and overseeing the implementation of the credit institution's ICT strategy as part of their overall business strategy as well as for the establishment of an effective risk management framework for ICT risks.
(3) A credit institution's management board shall ensure:
1) the sufficient number and skills of credit institution's staff to support their ICT operational needs and their ICT risk management processes and to ensure the implementation of their ICT strategy;
2) sufficient funds to fulfil the requirement referred to in the above item; and
3) appropriate training on ICT risks of staff members, including key function holders, on an annual basis, or more frequently if required.

ICT strategy
Article 5

(1) A credit institution shall:
1) adopt an ICT strategy;
2) define action plans that support the implementation of the ICT strategy; and
3) establish processes to monitor and measure the effectiveness of the strategy referred to in item (1) of this paragraph.
(2) A credit institution shall align the ICT strategy referred to in paragraph (1), item (1) of this Article with its overall business strategy, so that it covers:
1) how ICT should evolve to effectively support and implement the business strategy, including the evolution of the organisational structure, ICT system changes and key dependencies with third parties;
2) the planned strategy and evolution of the architecture of ICT, including third party dependencies; and
3) clear information security objectives, focusing on ICT systems and ICT services, staff and processes.
(3) In the action plan referred to in paragraph (1), item (2) of this Article, the credit institution shall define the activities to be taken to achieve the objective of the ICT strategy referred to in

paragraph (2) of this Article. The credit institution shall regularly review the action plans to ensure their relevance and appropriateness.

Use of third party providers
Article 6

(1) Without prejudice to the provisions of the Decision on outsourcing (Official Gazette 118/2020), a credit institution shall assess and reduce to an acceptable level the risks arising from contractual relationships with third parties whose activities are connected with the credit institution's ICT services and ICT systems.
(2) A credit institution shall ensure that contracts entered into with service providers provide for the continuity and security of ICT services and systems.
(3) The contracts referred to in paragraph (2) of this Article shall include the following:
1) appropriate and proportionate information security-related objectives and measures including minimum cybersecurity requirements, which includes specifications of the credit institutions' data life cycle, any requirements regarding the location of data centres, data encryption, network security and security monitoring processes; and
2) ICT incident handling procedures including escalation and reporting.
(4) A credit institution shall monitor and seek assurance on the level of compliance of service providers with the security objectives, measures and performance targets of the credit institution.

III ICT RISK MANAGEMENT FRAMEWORK

Organisation, objectives and ICT risk management procedure
Article 7

(1) A credit institution shall manage ICT risks to which it is or might be exposed, where the general rules for the implementation and setting up of a risk management system in terms of the Credit Institutions Act and the Decision on governance arrangements (Official Gazette 96/2018, 67/2019, 145/2020 and 145/2021) shall also apply to the ICT risk management.
(2) With the objective of setting up an effective ICT risk management, a credit institution shall define and assign key roles, define responsibilities and establish relevant reporting lines. The ICT risk management framework shall be fully integrated into, and aligned with, the credit institution's overall risk management framework.
(3) Within the ICT management framework, a credit institution shall put in place procedures to:
1) determine the risk appetite for ICT risks, in accordance with the risk appetite of the credit institution;
2) identify and assess the ICT risks to which a credit institution is exposed;
3) define risk mitigation measures;
4) monitor the effectiveness of these measures as well as the number of reported incidents, and take action to correct the measures where necessary;
5) report to the credit institution's management board on the ICT risks and measures; and
6) identify and assess whether there are any ICT risks resulting from any major change in ICT system or ICT services, processes or procedures, and/or after any significant ICT incident.
(4) A credit institution shall ensure that the ICT risk management framework is documented, and continuously improved, based on 'lessons learned' during its implementation and monitoring. The

ICT risk management framework shall be reviewed and approved, at least once a year, by the credit institution's management board.

Identification and classification of functions, processes and assets
Article 8

(1) A credit institution shall identify, establish and regularly maintain updated mapping of its business functions, roles and supporting business processes and information assets to identify the importance of each and their interdependencies related to ICT risks to be able to appropriately manage the information assets that support their critical business functions and processes.
(2) A credit institution shall clearly assign responsibility for the information assets.
(3) A credit institution shall classify the identified business functions, supporting processes and information assets referred to in item (1) of this Article in terms of their criticality, considering the confidentiality, integrity and availability requirements. A credit institution shall review the classification of the information assets, when risk assessment is performed.

ICT risk assessment and mitigation
Article 9

(1) A credit institution shall identify the ICT risks that impact the identified and classified business functions, supporting processes and information assets, according to their criticality.
(2) A credit institution shall carry out and document the ICT risk assessment annually or at shorter intervals in the event of any major changes in infrastructure or procedures affecting the business functions, supporting processes or information assets.
(3) A credit institution shall continuously monitor threats and vulnerabilities relevant to their business processes, supporting functions and information assets and regularly review the risk scenarios impacting them.
(4) Based on the ICT risk assessment results, a credit institution shall define and implement measures to mitigate the identified ICT risk, ensure that this risk stays within the credit institution's risk appetite and protect information assets in accordance with their classification.
(5) ICT risk assessment results shall be reported to the credit institution's management board in a clear and timely manner.

ICT audit
Article 10

(1) The internal audit function shall, complying with the requirements prescribed by the Decision on governance arrangements and following a risk assessment approach, carry out independent audit and provide objective assurance of the compliance of all activities and organisational units in ICT and security, with the credit institution's policies and procedures.
(2) Internal auditors with sufficient knowledge, skills and expertise in ICT risks shall carry out regular audits of the credit institution's governance, ICT risk-related systems and processes/procedures to provide independent assurance of their effectiveness to the credit institution's management board.
(3) A credit institution's management board shall approve the internal 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 ICT risks in the credit institution and shall be updated regularly.
(4) A credit institution shall establish a formal follow-up process to monitor proposals, recommendations and measures for their remediation in order to remedy any material irregularities and deficiencies established by ICT audit findings.

IV INFORMATION SECURITY

Information security policy
Article 11

(1) A credit institution shall develop and document an information security policy that shall define the principles and rules to protect the confidentiality, integrity and availability of the credit institution's and its customers' information. The information security policy shall be in line with the credit institution's information security objectives and based on the relevant risk assessment results. The policy shall be approved by the credit institution's management board.
(2) The information security policy shall include a description of the main roles and responsibilities of information security management. A credit institution shall ensure that the information security policy is appropriately communicated to all staff and third parties.
(3) Based on the information security policy, a credit institution shall establish and implement security measures to mitigate the ICT risks that it is exposed to. These measures shall include:
1) governance controls;
2) logical controls;
3) physical controls;
4) ICT operations security;
5) security monitoring;
6) information security reviews, assessment and testing; and
7) information security training and awareness.

Information security manager
Article 12

A credit institution's management board shall set up the function of information security manager, which shall be independent of the function of ICT organisational unit manager, and shall define his/her scope of activity, authority and responsibilities.

Logical security
Article 13

A credit institution shall define, document, implement, monitor and regularly review the procedures for logical access control. The procedures shall also include controls for monitoring deviations and anomalous activities. These procedures shall take into consideration and, where applicable, implement the following:
(1) need to know basis principle, the principle of least privilege and the principle of segregation of duties;
(2) unambiguous identification and the possibility to determine user responsibility for the access and the actions performed in the ICT systems;

(3) appropriate assignment of and control over privileged access;
(4) appropriate logging of user activities;
(5) access management process which, according to the business need, includes appropriate procedures of granting, assignment, review, modification or withdrawal of access rights; and
(6) authentication methods that are sufficiently reliable and commensurate with the criticality of ICT systems, information or processes being accessed.

Physical security
Article 14

(1) A credit institution shall define, document and implement physical security measures to protect its premises, data centres and other sensitive areas from unauthorised access and from environmental hazards.
(2) A credit institution shall only permit physical access to ICT systems to authorised individuals. Authorisations shall be assigned in accordance with the individual's roles and responsibilities and limited to individuals who are appropriately trained and whose activities are appropriately monitored. Physical access shall be regularly reviewed to ensure that unnecessary access rights are promptly revoked when not required.

ICT operations security
Article 15

(1) A credit institution shall implement procedures to prevent the occurrence of security issues in ICT systems and services and shall minimise their impact on ICT service delivery. These procedures shall include the following measures:
1) identification and remedy of potential vulnerabilities by ensuring that software and firmware are up to date, by deploying critical security patches or by implementing compensating controls;
2) implementation of secure configuration baselines of all network components;
3) in accordance with the carried out risk assessment and data classification, the implementation of network segmentation, data loss prevention systems and the encryption of network traffic;
4) implementation of protection of endpoints of ICT systems, including servers, workstations and mobile devices;
5) in accordance with the carried out risk assessment, ensuring that mechanisms are in place to verify the integrity of software, integrated firmware and data; and
6) in accordance with the data classification, encryption of data at rest and in transit.
(2) On an ongoing basis, a credit institution shall determine whether changes in the existing operational environment influence the existing security measures or require adoption of additional measures to mitigate related risks.

Security monitoring
Article 16

(1) A credit institution shall establish the process and implement procedures to detect anomalous activities that may impact the credit institution's information security and to respond to these events appropriately. As part of this continuous monitoring, a credit institution shall implement appropriate and effective mechanisms for detecting physical and logical intrusion as well as breaches of confidentiality, integrity and availability of the information assets.

(2) A credit institution shall establish processes and implement procedures to identify and constantly monitor security and operational threats that could materially affect the credit institution's abilities to provide services. A credit institution shall actively monitor technological developments to ensure that it is aware of security risks.

Information security reviews, assessment and testing
Article 17

(1) A credit institution shall review, assess and test information security to ensure the effective identification of vulnerabilities in its ICT systems and services.
(2) A credit institution shall establish and implement an information security testing framework that considers threats and vulnerabilities, identified through threat monitoring and ICT risk assessment.
(3) A credit institution shall use the information security testing framework to ensure that tests:
1) 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 that are tested; and
2) include vulnerability scans and penetration tests commensurate to the level of risk identified with the business processes and ICT systems.
(4) A credit institution shall perform ongoing tests of the security measures, which includes the following:
1) for all critical ICT systems at least on an annual basis; and
2) for non-critical ICT systems, using a risk-based approach, at least once every three years.
(5) A credit institution shall ensure that tests of security measures are conducted in the event of significant changes to processes, infrastructure and internet-facing applications.
(6) A credit institution shall monitor and evaluate the results of the conducted security tests and update its security measures accordingly without undue delays in the case of critical ICT systems.
(7) Tests of the security measures shall take into consideration the scenarios of relevant and known potential attacks.

Information security training and awareness
Article 18

A credit institution shall establish a training programme, including periodic security awareness programmes, for all of its staff and third parties to ensure that they are trained to perform their duties and responsibilities consistent with the relevant security policies and procedures. A credit institution shall ensure that the training programme provides training for all staff members and third parties at least annually.

V ICT OPERATIONS MANAGEMENT

ICT operations management procedures
Article 19

(1) A credit institution shall manage its ICT operations based on documented, adopted and implemented processes and procedures. These documents shall define how the credit institution operates, monitors and controls its ICT systems and services.
(2) A credit institution shall ensure that performance of its ICT operations is aligned to their business requirements. A credit institution shall maintain and improve efficiency of its ICT operations, mainly to minimise errors arising from the execution of manual tasks to the least possible measure.
(3) A credit institution shall record, monitor and keep logs for critical ICT operations to allow the detection, analysis and correction of errors.
(4) A credit institution shall maintain an up-to-date inventory of its ICT assets and ensure a sufficiently detailed inventory to:
1) enable the prompt identification of an asset, its security classification, its location and ownership and interdependencies between different assets;
2) enable proper configuration and change management processes; and
3) help in the response to incidents.
(5) A credit institution shall:
1) monitor and manage the life cycles of ICT assets, to ensure that ICT assets are aligned with business and risk management requirements;
2) monitor whether its ICT assets are supported by third parties and staff in charge of internal development and whether all relevant patches and upgrades are applied; and
3) assess and mitigate the risks stemming from outdated or unsupported ICT assets.
(6) A credit institution 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.
(7) A credit institution shall:
1) define and implement data and ICT systems backup and restoration procedures to ensure that they can be recovered as required;
2) set the scope and frequency of backups according to the risk assessment, business recovery requirements and the criticality of the data and the ICT systems; and
3) regularly test the backup and restoration procedures.
(8) A credit institution 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.

Incident and problem management
Article 20

(1) A credit institution shall establish appropriate processes and organisational structures to ensure a consistent and integrated controls of incidents and problems, handling and their follow-up. Under incident and problem management the credit institution shall include the following:
1) the procedures to identify, track, log, categorise and classify incidents according to a priority, based on business criticality;
2) the roles and responsibilities for different incident scenarios (e.g. errors, malfunctioning, cyber-attacks);
3) problem management procedures to identify, analyse and solve the root cause behind one or more incidents in order to prevent the incident from repeating;
4) 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;

5) effective internal communication plans, including incident notification and escalation procedures; and
6) specific communication plans for critical business functions and processes in order to collaborate with relevant stakeholders and provide timely information to external parties.
(2) In the event of major ICT incidents, a credit institution shall, within an appropriate timeframe from the occurrence of the incident, notify the Croatian National Bank of the incident, its effects and the actions taken.

VI ICT PROJECT AND CHANGE MANAGEMENT

ICT project management
Article 21

(1) A credit institution shall set up a project governance process that defines roles and responsibilities required to effectively support the implementation of the ICT strategy.
(2) A credit institution shall appropriately monitor and mitigate risks deriving from ICT project 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.
(3) A credit institution shall establish and implement an ICT project management policy that includes as a minimum:
1) project objectives;
2) roles and responsibilities;
3) a project risk assessment;
4) a project plan, timeframe and steps;
5) key milestones; and
6) change management requirements.
(4) A credit institution shall, through the ICT project management policy, ensure that information security requirements are analysed and approved by a function that is independent from the development function.
(5) A credit institution 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.
(6) Depending on the importance and size of the ICT projects, a credit institution shall report on the establishment and progress of ICT projects and their associated risks to the management board regularly and on an ad hoc basis as appropriate.

ICT systems acquisition and development
Article 22

(1) A credit institution shall define and implement a process, designed using a risk-based approach, governing the acquisition, development and maintenance of ICT systems.
(2) A credit institution 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 management level.

(3) A credit institution shall ensure that measures are in place to mitigate the risk of unintentional alteration or intentional manipulation of the ICT system during development and implementation in the production environment.
(4) A credit institution shall:
1) define a methodology for testing and approval of ICT systems prior to their first use, considering the criticality of business processes and assets;
2) use test environments that adequately reflect the production environment; and
3) confirm by the testing that new ICT systems perform as intended.
(5) A credit institution shall test ICT systems, ICT services and information security measures to identify potential security weaknesses, deviations and incidents.
(6) A credit institution shall:
1) implement separate ICT environments to ensure adequate segregation of duties and to mitigate the impact of unverified changes to production systems;
2) ensure the segregation of production environments from development, testing and other non-production environments;
3) protect the integrity and confidentiality of production data in non-production environments and restrict access to production data to authorised users; and
4) protect the integrity of the source codes of ICT systems that are developed in-house.
(7) A credit institution shall document the development, implementation, operation and configuration of the ICT systems comprehensively.
(8) In accordance with the risk assessment, a credit institution shall also apply processes for acquisition and development of ICT systems to ICT systems developed or managed by the business function's end users outside the ICT organisation. The credit institution shall maintain a register of such systems that support critical business functions or processes.

ICT change management
Article 23

A credit institution 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.

VII BUSINESS CONTINUITY MANAGEMENT

General provisions on business continuity management
Article 24

The process of business continuity management shall be subject to the provisions of the Decision on governance arrangements, unless otherwise prescribed by this Decision.

Business impact analysis
Article 25

(1) A credit institution shall regularly conduct business impact analysis (BIA) to include the potential impacts of business disruptions on confidentiality, integrity and availability and consider

the criticality and interdependencies of business functions, supporting processes, third parties and information assets.
(2) A credit institution shall ensure that its ICT systems and services are aligned with its BIA.

Recovery plans
Article 26

(1) A credit institution shall, based on the BIA and plausible scenarios, adopt recovery plans providing for the recovery and availability of ICT systems and services necessary for the carrying out of critical and/or vital business processes within a data recovery time objective and a recovery point objective.
(2) Within the framework of the recovery plans, a credit institution shall consider and implement continuity measures to mitigate the cases of disruptions of availability of third parties, which are of key importance for the credit institution's ICT service continuity.

Testing of plans
Article 27

(1) A credit institution shall test its ICT systems' recovery plans regularly, and at least once a year the recovery plans for ICT systems and services required for the carrying out of vital/critical business functions and processes.
(2) Based on testing results, current threat intelligence and lessons learned from previous events, a credit institution shall update its business continuity plans and recovery plans at least once a year. Any changes in recovery objectives, business functions, supporting processes or information assets shall also be a basis for updating the business continuity plans and recovery plans.
(3) The credit institution's testing of its recovery plans shall demonstrate that it is able to sustain the viability of its businesses until critical operations are re-established. By this testing, the credit institution shall in particular:
1) include testing of an adequate set of severe but plausible scenarios including those considered for the development of the business continuity plans and recovery plans;
2) in accordance with the risk assessment, include the switch-over of critical business functions and supporting processes in the disaster recovery environment and demonstrate that they can be run in this way for a sufficiently representative period of time and that normal functioning can be restored afterwards;
3) design the tests to challenge the assumptions on which business continuity plans rest (including crisis governance arrangements and crisis communication plans) as well as ICT systems' recovery plans; and
4) verify the ability of its staff and third parties, ICT systems and services to respond adequately to the scenarios and recovery objectives.
(4) A credit institution shall:
1) document test results; and
2) analyse any identified deficiencies resulting from the tests and report them to the credit institution's management board.

Crisis communications
Article 28

In the event of a disruption of operation or other crisis events and during the implementation of the business continuity plans and recovery plans, a credit institution shall ensure effective crisis communication measures so that all relevant internal and external stakeholders (including the competent authorities and third parties) are informed in a timely and appropriate manner.

VIII TRANSITIONAL AND FINAL PROVISIONS

Entry into force and application
Article 29

(1) On the date of the entry into force of this Decision, the Decision on adequate information system management (Official Gazette 37/2010) shall cease to have effect.
(2) This Decision shall be published in the Official Gazette and shall enter into force on 1 April 2023.
(3) When first amending existing arrangements with third parties whose activities are related to ICT services and ICT systems and by 31 December 2023 at the latest, a credit institution shall, in accordance with the risk assessment, review and, where necessary, amend existing arrangements with a view to ensuring their compliance with this Decision.

No.: 321-091/09-22/BV
Zagreb, 9 September 2022

Governor
Boris Vujčić