Recommendation 8/2020. (VI.22.) of the Magyar Nemzeti Bank on the protection of information systems

TRANSLATION

I. OBJECTIVE AND SCOPE OF THE RECOMMENDATION

The protection of information systems should be a priority for the members of the financial intermediary system in order to protect their own and their customers' assets entrusted to their care, as well as all their data, which are suitable to directly identify or indirectly refer to the customer, their habits, special situation (hereinafter: customer data) – and their tax, trade, banking, securities, fund, payment, insurance or occupational pension secrets (henceforth: financial sector secret). In addition to the provisions of sectoral laws[1] pertaining to certain financial activities, a separate government decree (hereinafter: Government Decree)[2] regulates the protection of information systems of financial institutions, insurance and reinsurance companies, as well as investment companies and commodity exchange service providers.

The objective of this guideline is to provide practical guidance to the members of the financial intermediary system on establishing the protection of their information systems in a risk proportionate manner, and on the uniform interpretation of legal provisions regulating their protection. The recommendation primarily outlines the rules of the Government Decree out of the legal provisions defining certain topics and frameworks, the wording of the sectoral laws may differ slightly from this. The recommendation defines the expected measures based on the risks arising in the areas of protection specified in the legal provisions, and proposes best practices for meeting expectations (hereinafter: "exemplary practices"). Implementing all exemplary practices concurrently is not always practical, because they can act as compensating controls of each other. Expectations can be met by other solutions as well, provided that the risk mitigation objective of the given expectation is met.

The recommendations are based on the experience of supervisory reviews and the known and reasonably expected requirements of general IT security at the time of issue.

The legal provisions also allow members of the financial intermediary system to perform IT activities only partially by themselves, the activities may be outsourced in part or entirely on condition that the ultimate responsibility for the outsourced activities rests with the institution. The guideline also addresses the IT security aspects of outsourcing, in line with the legal provisions.

---

[1] Act CCXXXVII of 2013 on credit institutions and financial enterprises; (henceforth: Hpt.) 67. §, subsection (1), paragraph d), and 67/A. §,
Act CCXXXV of 2013 on certain payment service providers; 12. §, subsection (1), paragraph d), and subsection (3), also 12/A. §,
Act CXXXVIII of 2007 on investment companies and commodity exchange service providers, and on the rules of their activities (henceforth: Bszt.) 12. §,
Based on Act CXX of 2001 on the capital market 318/D. §, Bszt. 12. §,
Act XVI of 2014 on Collective Investment Trusts and Their Managers, and on the Amendment of Financial Regulations; 29. § and 30. §,
Act LXXXII of 1997 on private pension and private pension funds; (henceforth: Mpt.) 77/A. §,
Act XCVI of 1993 on voluntary mutual insurance funds; (henceforth: Öpt.) 40/C. §,
Act LXXXVIII of 2014 on insurance activities; 94. §, subsection (1), paragraph c) and subsections (3)-(6)

[2] Government Decree 42/2015 (III. 12.) on the protection of the information systems of financial institutions, insurance and reinsurance companies, as well as investment companies and commodity exchange service providers

The addressees of this recommendation are organizations and persons (henceforth collectively: institution) subject to the laws specified in Section 39. of the Act CXXXIX of 2013 on the Magyar Nemzeti Bank (hereinafter: MNB tv.).

The recommendation should be applied together with the MNB Recommendation 4/2019 (IV. 1.) on the usage of community and public cloud computing services[3], the Executive circular on written contracts and written declarations concluded by electronic means[4], MNB Recommendation 27/2018 (XII. 10.) of the MNB on internal defence lines and the governance and control functions of financial institutions and the MNB Recommendation on the use of external service providers[5].

This guideline does not comprehensively refer to legal provisions when defining principles and expectations, but the addressees of the recommendation are of course still required to comply with relevant legal requirements.

This recommendation does not define guidance regarding the handling of data and data protection matters, does not contain any requirements regarding the handling of personal data, and the requirements contained therein shall in no way be understood as an authorisation for processing of personal data. Handling of data in relation to the fulfilment of supervisory requirements set out in these recommendations may be carried out exclusively in compliance with the legal provisions on data protection in force at any time.

II. PLANNING, ORGANISATION, POLICIES AND RISK ASSESSMENT

1. IT PLANNING AND ORGANIZATION

1.1. Documents of corporate IT governance and planning

1.1.1. Pertinent legal provisions: *The requirements associated with information technology, along with the rules relating to the assessment and management of the security risks resulting from its use in the areas of IT corporate governance, planning, development and acquisition, as well as operation, monitoring and independent audit, shall be defined in the management system.[6] The institution shall have procedures and provisions relating to the operation of its information system, as well as plans for the development thereof*.[7]

1.1.2. IT costs, investments, developments serve business goals and needs, and the purpose of IT control measures is to reduce the risks assessed based on business processes to an acceptable level. IT investments do not serve a purpose by themselves, they serve business processes or their risk proportionate protection in all cases, directly or indirectly. Therefore, the institution defines the rules of IT (corporate) governance and planning based on its business strategy, as follows:

1.1.3. The policies on corporate IT governance and planning conform to the institution's business goals, by taking into account the IT, data communication technology and information security trends. The institution prepares at least the following documents during IT planning:

---

[3] https://www.mnb.hu/letoltes/4-2019-cloud-bg.pdf in English, https://www.mnb.hu/letoltes/4-2019-felho.pdf in Hungarian

[4] https://www.mnb.hu/letoltes/ejognyil-korlevel.pdf

[5] Under preparation

[6] Bszt. 12. §, subsection (2), Mpt. 77/A. §, subsection (1), Öpt. 40/C. §, subsection (1), Gov. Decree 2. §, subsection (1)

[7] Bszt. 12.§, subsection (7), paragraph a), Mpt. 77/A. §, subsection (6), paragraph a), Öpt. 40/C. §, subsection (6), paragraph a), Gov. Decree 3. §, subsection (3), paragraph a)

a) IT strategy,

b) annual plans of IT investments and costs.

1.1.4. For the adequate application of information security principles, the IT strategy documents are always prepared with the involvement and approval of the information security function.

1.1.5. With regards to the desired goals, the institution defines at least the expected and desired states for IT infrastructure, architecture, operations, the most important applications serving the business areas and outsourcing in its IT strategy.

1.1.6. The institution follows up the achievement of the goals of the IT strategy regularly, but at least annually, in line with the strategy's time span, in a documented manner. The institution assesses any deviations from the strategy.

1.2. Organisational and operational requirements

1.2.1. Pertinent legal provisions*: The institution shall define the organisational and operational requirements by taking into account the security risks deriving from the use of information technology, roles and responsibilities, procedures for record keeping and communication.*[8]

1.2.2. The institution defines the structure of its IT organisation in organisational and operational requirements, and assigns the roles and responsibilities to IT job roles in documents that verify that they had been accepted by the employees (e.g. job descriptions).

1.2.3. The institution establishes its IT organisation, responsibilities, and its operating procedures, record keeping and communication rules.

1.2.4. The institution establishes the information security function, or organisation and respective roles in a way that is proportionate to the information security risks, and provides for at least the following aspects of the information security function:

a) clearly defines its roles and responsibilities;

b) establishes the function's adequate organisational independence and direct accountability to the management body;

c) defines and excludes the function's incompatible duties, or separates them with the application of appropriate control measures;

d) periodic review of the adequacy of the function's expertise and activity;

e) continuous education.

1.2.5. Information security is the responsibility of the most senior operational officer (executive), who can delegate this role.

2. INFORMATION SECURITY MANAGEMENT SYSTEM

2.1. The principles of information security management system

2.1.1. Pertinent legal provisions: *The institution shall set up its policy system related to the security of the information system used for performing its financial services, auxiliary financial services, insurance and reinsurance and directly related activities, as well as investment service activities and auxiliary services,*

[8] Bszt. 12. §, subsection (4), Mpt. 77/A. §, subsection (3), Öpt. 40/C. §, subsection (3), Gov. Decree 2. §, subsection (3)

and ensures the risk proportionate protection of the information systems. The policy system shall specify the requirements associated with information technology and the rules related to the assessment and management of the security risks arising from its use in the areas of corporate IT governance, planning, development and acquisition, as well as operation, monitoring and independent audit.[9]

2.1.2. The policy system encompasses the continuous definition, introduction, compliance, adherence (enforcement), sanctioning, monitoring, review and update of behaviour patterns to be followed, rules and processes, as well as the rectification of deficiencies found in the course of reviews, and the respective procedures, documentation, formal approval procedures, and the communication thereof to stakeholders (publication).

2.1.3. The information security management system is the system of policies related to the protection of telecommunication and data communication systems, and the secure operation of systems. Its objective is to reduce the IT related operational risks resulting from undesired activity, lack of information and failure to document the performed activities. A suitable information security management system is an indirect and preventative control of the institutions' information security, its comprehensiveness and continuous adequacy ensures the accountability for the expected behaviour and performance at the institution.

2.1.4. When establishing the information security management system, the institution ensures that its policy system conforms to the nature of its financial activity, stays in proportion with its magnitude and complexity, and complies with the measures ensuring the risk proportionate protection of the information system.

2.1.5. The institution ensures that its risk proportionate administrative protection measures are based on the identification and classification of the data, information, and IT assets to be protected, and the risks threatening them. These measures contain institution specific detailed rules, which can be derived from the existing regulatory environment.

2.1.6. The institution brings into force the policies according to the procedures defined in the policy system in a documented way, communicates them to those falling into its personal scope, and documents it, and clearly defines the availability of policies in force.

2.1.7. The institution regulates the frequency, the persons responsible and the procedures for documenting the review and updating of policies within the policies or in the policy governing the system of policies. The institution reviews and updates the policies upon each significant change in legislation, policies, application environment or work process, but latest as part of the regular review of information security.

2.1.8. The provisions of the policy system's elements are straightforward, clear, easy to understand, feasible and enforceable.

2.1.9. When establishing policies, the institution defines policies' material, personal and geographic scope with special attention to making them applicable and available only to those, for whom it is absolutely necessary.

2.1.10. When establishing the information security management system, the institution may take into consideration industry standards, guidelines, methodologies, but the MNB expects that policies always befit the operations of the institution. Policies shall not prescribe practices that are irrelevant,

[9] Bszt. 12. §, subsections (1) and (2), Mpt. 77/A. §, subsection (1), Öpt. 40/C. §, subsection (1), Gov. Decree 2. §, subsection (1)

unrealistic, technically unfeasible, disproportionate to risks, not in accordance with the operations of the institution, or unenforceable.

2.2. The security classification system

2.2.1. Pertinent legal provisions: *The institution shall at all times have a security classification system for the elements of the information system.*[10]

2.2.2. The data owner classifies data into data security classes based on security risks concerning their confidentiality, integrity, and availability. The data owner – in proportion to the risks – defines at least the security conditions, rules, and procedures of data access, transfer, storing, archiving, deleting, destruction, physical access protection, labelling, encryption and transporting. The data owner assigns the elements serving the business processes using the data into protection classes, based on the classification of the impacted data – by taking into account not only hardware and software elements, but also telecommunication and data communication systems, as well as organisations taking part in the processing of the data and their infrastructure. The system comprehensively established according to this point is the security classification system.

2.2.3. The institution regulates the rules and procedures of the security classification system in its information security management system.

2.2.4. The institution's security classification system complies with the legal provisions on financial sectoral secrecy and protection of personal data, and the institution's data protection provisions.

2.2.5. The institution assigns customer data and financial sector secrets (including sensitive payment data), and the data derived from them in a decryptable manner, as well as the systems and elements of infrastructure processing them into the strictest security class.

2.2.6. The institution may define a security class even stricter than the one defined in point 2.2.5., if the assigned security measures clearly name the natural persons having access to the data.

2.3. Document containing the appointment of system owner and data owner

2.3.1. Pertinent legal provisions: *The institution shall at all times maintain the document containing the appointment of the data owner and the system owner.*[11]

2.3.2. The data owner and the system owner are important elements of enforcing information security. The data owner defines the confidentiality, integrity and availability requirements of data entrusted to his/her care, including the security class of data, the access, modification, deletion, storage and other rights to data, other security requirements, and the rules of storing, saving, archiving, transferring and deleting data. The system owner enforces the protection measures defined by the data owner by technological means.

2.3.3. The institution regulates the roles and responsibilities of data owners and system owners, the procedures of appointing them and the performance of their tasks, and the documentation thereof.

2.3.4. The institution defines the role of the data owner to include at least the tasks of classifying data assets entrusted to his/her care, defining the access, modification, deletion, storage and other rights to data,

[10] Bszt. 12. §, subsection (9), paragraph c), Mpt. 77/A. §, subsection (7), paragraph c), Öpt. 40/C. §, subsection (7), paragraph c), Gov. Decree 4. §, subsection (1), paragraph c)
[11] Bszt. 12. §, subsection (9), paragraph e), Mpt. 77/A. §, subsection (7), paragraph e), Öpt. 40/C. §, subsection (7), paragraph e), Gov. Decree 4. §, subsection (1), paragraph e)

as well as defining security requirements, and the procedures of data storage, backup, archiving, transfer and deletion.

2.3.5. The institution appoints those natural persons, who perform the data owner and system owner tasks, and designates the information assets entrusted to their care in a clear and accountable manner.

2.3.6. The institution informs the data owners and system owners of their appointment, roles and responsibilities according to the approved procedure and in a documented way.

2.3.7. The institution ensures the verifiability of the data owners and system owners accepting their appointments, roles and responsibilities.

2.3.8. The institution involves the impacted data oner(s) in the development its information systems and business processes.

2.4. IT skills required for job roles

2.4.1. Pertinent legal provisions: *In its internal rules the institution shall specify the IT skills needed for occupying specific job posts.*[12]

2.4.2. The institution ensures that employees possess adequate skills to protect the confidentiality, integrity and availability of data related to business processes.

2.4.3. The institution defines and lists in detail the specific IT – including information security – skills required to fill any given business and IT job role.

2.4.4. The institution ensures that roles are filled by persons who possess the expected and up-to-date skills.

3. INFORMATION SECURITY RISK ASSESSMENT, THE RISK PROPORTIONATE PROTECTION OF THE INFORMATION SYSTEM

3.1. Risk assessment

3.1.1. Pertinent legal provisions: *The institution shall ensure the protection of the information system commensurate with the risks incurred. The policy system shall define the requirements associated with information technology, and the rules of assessing and managing the security risks arising from its use in the areas of IT corporate governance, planning, development and acquisition, as well as operation, monitoring and independent audit.*[13] *The institution reviews and updates the information system's security risk assessment as necessary, but at least every two years.*[14] *In order to perform the institution's activities and to keep its records in a timely and secure manner, the institution implements the protective measures, which are justified by the risk assessment.*[15] *Risk proportionate protection: protection of the electronic information system, with the costs of protection in proportion with the damages potentially caused by the threats.* [16]

3.1.2. Risk assessment consists of risk analysis (the identification and classification of risks), and the planning of risk mitigation measures. The risk management process consists of risk assessment, and the implementation, review and correction of planned risk mitigation measures.

---

[12] Bszt. 12. §, subsection (11), Mpt. 77/A. §, subsection (9), Öpt. 40/C. §, subsection (9), Gov. Decree 5. §
[13] Bszt. 12. §, subsections (1) and (2), Mpt. 77/A. §, subsection (1), Öpt. 40/C. §, subsection (1), Gov. Decree 2. §, subsection (1)
[14] Bszt. 12. §, subsection (3), Mpt. 77/A. §, subsection (2), Öpt. 40/C. §, subsection (2), Gov. Decree 2. §, subsection (2)
[15] Bszt. 12. §, subsection (7), Mpt. 77/A. §, subsection (6), Öpt. 40/C. §, subsection (6), Gov. Decree 3. §, subsection (3)
[16] Gov. Decree 3. §, subsection (3), paragraph c)

3.1.3. The institution prepares an information security risk assessment and management policy, which regulates at least the rules and procedures of assessing and managing institution specific security risks that arise from the applied information technology, in the following fields of IT:

a) (corporate) governance,
b) planning, system development and acquisition,
c) operations,
d) monitoring,
e) independent review.

3.1.4. Risk assessment serves as a basis for implementing risk proportionate protection, to which legal provisions attach great importance: they subject a significant part of the protection measures expected from the institution to conditions that are justified by a risk assessment, and are in proportion with the potential damages caused by the threats. If the institution does not have an adequate, institution specific risk assessment that reveals the relevant threats, then the legal compliance of its risk assessment process cannot be substantiated. Therefore, the MNB in its supervisory role of the financial intermediary system pays particular attention to that the risk assessment is documented, up-to-date, and relevant to the institution.

3.1.5. Pertinent laws do not regulate the details for performing risk assessments (e.g. methodology, processes, steps), the institution decides about them at its own discretion. The MNB expects that the risk assessment primarily takes into account the specifics of the institution, therefore generic risk assessment methodologies shall be relied upon only as a guidance, because they may also contain such threats that are not relevant to the institution, and relevant threats may be defined too broadly or omitted. The costs of security measures which are planned by using generic risk assessments, or risk assessments optimised for other institution(s), and the damages potentially caused by respective risks may be out of proportion, or may not respond to the relevant threats, therefore do not meet the legal provisions.

3.2. Risk analysis

3.2.1. The institution prescribes in its information security management system the mandatory, regular assessment of the security risks relevant to its information systems, designates the responsible person for assessing the risks, and defines the rules for carrying out the assessment and the subsequent activities.

3.2.2. The institution identifies the security risks of its IT system with due care and in a fully comprehensive manner in all areas relevant to information security (e.g. IT (corporate) governance, planning, development, acquisition, operations, monitoring, independent review).

3.2.3. The institution classifies the relevant risks that were identified during the risk assessment based on their probability and impact.

3.2.4. The institution documents and approve the results of the risk assessment – including the classification – according to its information security policies.

3.2.5. The institution performs the following steps at least during the risk assessment:

a) selection, interpretation and documentation of the methodology;

b) identification of business processes, including the assessment and classification of data, the risk classification of processes based on the confidentiality, integrity and availability requirements of data and processes;

c) identification and selection of business critical, main processes;

d) the identification and documentation of the information technology and data communication system elements, and information security vulnerabilities of processes, such as manual data entry and modification, data transfers between systems, remote accesses, technical accesses, shared data, temporary data files, software vulnerabilities, and scaling of architecture;

e) performing reviews on the existence and effective operating of information security controls related to system elements and vulnerabilities, and thereby the identification of security deficiencies and inadequacies, as well as the assessment and documentation of risks;

f) review and assessment of general information security controls (i.e. controls not linked directly to system elements, such as human resources, policies, security measures of the infrastructure), whereby the institution may take into account recommendations and catalogues issued by professional bodies[17], and good practices;

g) review of the compliance of practices to policy requirements;

h) creating an information security overview of the institution's critical IT environment, and preparing the risk assessment report;

i) in the risk assessment report the institution produces a complete record of the processes reviewed, the elements of the system, the identified vulnerabilities, the security measures subject to the review, the findings, the extent of the risks, as well as the relevant circumstances to the assessment. Thereby the document enables the performance of retrospective reviews, sets out the scope of the assessment, and may also provide a starting point for the risk assessment of the following period;

j) following the identification of the risks, the organisational units assessing the risk and being reviewed consult in order to reveal any potential false findings and differing views on the evaluation of risks;

k) the risk assessment report – at least in the form of a management summary – is discussed and approved by the management body of the institution.

3.3. Managing the identified risks

3.3.1. The institution documents and approves an action plan to manage the risks identified and classified during the risk assessment. The risks, which are not managed, are accepted by management in a documented manner. The acceptable extent (i.e. risk appetite) and rules of risk acceptance are defined in advance. The institution may not accept risks that violate legal provisions or regulatory requirements.

3.3.2. The institution defines specific tasks in the action plan, which are clearly assigned to the risks identified, and substantially reduces their extent, as well as assesses the resources required.

[17] e.g. COBIT5, MSZ/T ISO/IEC 27001:2014, BSI IT-Grundschutz-Kataloge

3.3.3. The institution manages the execution of the tasks by setting clear deadlines – in proportion to the extent of the risk, and the resources required –, as well as designates the person(s) responsible. The deadlines cannot exceed the scheduled date of the subsequent risk assessment.

3.3.4. The action plan is approved by the manager or management body designated by the policies of the institution in a documented manner. The decision states that the management body has familiarised itself with the results of the risk assessment, and accepts those risks that were identified, but do not constitute part of the action plan.

3.3.5. The institution tracks and reviews the execution of the tasks in the action plan by the designated person(s) responsible. In case the execution deviates from the action plan the institution brings corrective measures to complete the tasks by the deadline, and according to plan.

3.3.6. The institution documents the accepted risks, and reviews them according to the intervals specified in its information security management system, but latest during the subsequent risk assessment.

3.4. The review of the risk assessment

3.4.1. In case of changes to the business processes, the information system, the relevant regulations or policies the institution reviews its risk assessment in the areas impacted by the change immediately and updates it in a documented manner.

3.4.2. The institution updates its risk assessment in a fully comprehensive and documented manner, every two years or more frequently, encompassing all areas of information security.

III. ACQUISITION, DEVELOPMENT, TESTING, CHANGE MANAGEMENT

4. COMMON PROVISIONS

4.1.1. Pertinent legal provisions: *The regulatory system shall specify the requirements associated with information technology and the rules relating to assessing and managing the security risks involved in its use in the field of IT corporate governance, planning, development and acquisition, as well as operation, monitoring and independent audit.*[18]

4.1.2. The financial institution may outsource the acquisition and development of systems and services to external contractors relating to the performance of its services or auxiliary services. The financial institution remains responsible for the procured systems, activities and developments.

4.1.3. The financial institution - develops an IT (corporate) governance solution, regulated by its information security management system, that allows the continuous documented monitoring of simultaneous IT projects and the managing of the risks identified during the course of the projects or arising from inter-project dependencies, and also comprehensively defining and implementing the roles and responsibilities of experts.

4.1.4. The financial institution ensures that the IT security function is continuously involved in procurements and developments throughout their entire lifecycle, beginning from their planning and design, with such rights that allow the evaluation of the suitability of specifications prior to procurement or development, as well as checking their changes that take place during the process; determining and

[18] Bszt. 12. §, subsections (1) and (2), Mpt. 77/A. §, subsection (1), Öpt. 40/C. §, subsection (1), Gov. Decree 2. §, subsection (1)

extending specific security and control functions and monitoring their development, and giving expert opinion thereon.

4.1.5. In order to reduce the risks of acquisition and development the financial institution performs the following activities:

4.2. Acquisition

4.2.1. Pertinent legal provisions: *the acquisition of the systems and services shall be controlled, monitored, and complies with the security prescriptions.*[19]

4.2.2. The institution defines the rules and procedures of acquisition in its information security management system.

4.2.3. The institution defines the mandatory contractual elements in its information security management system for the acquisition of systems and services – for each contract types.

4.2.4. In case of service contracts (hereinafter: SLA) the institution applies contractual terms that ensure the service can be measured, enforced, and sanctioned by the institution (enforcing the SLA requirements.

4.2.5. The institution ensures by contractual terms, that upon termination of the contract the service provider hands over the data it manages or processes either directly or indirectly, in a format that can be processed by using technology independent from the provider.

4.2.6. Exemplary practices

The institution may specify in the contracts that measuring the level of service is performed by the institution itself or by an independent external expert on behalf of the institution, because the SLA conformity cannot be controlled by the institution if the measurement is conducted by the service provider and conformity is reported by them at a later point, therefore performance not in conformity with the contract, which cannot be substantiated, may cause direct and indirect damages to the institution.

4.3. Development

Pertinent legal provisions: *The institution shall have every document in its possession that ensures the continuous and secure operating of the information systems that directly or indirectly support its business activity, even after the supplier or the developer of the system ceases to exist.*[20] *The institution shall, at all times, have the system descriptions and models in its possession, which are necessary for reviewing the structure and operating of the information system developed or commissioned by the institution, and the syntax rules of the data and the data storage structure within the information system developed or commissioned by the institution.*[21]

4.3.1. During in-house developments or developments with the involvement of an external developer the financial institution ensures and records in its information security management system - that the system development documentation of the installed systems:

a) is produced in a clear format;

---

[19] Gov. Decree 5/B. §, paragraph l)

[20] Bszt. 12. §, subsection (7), paragraph b), Mpt. 77/A. §, subsection (6), paragraph b), Öpt. 40/C. §, subsection (6), paragraph b), Gov. Decree 3. §, subsection (3), paragraph b)

[21] Bszt. 12. §, subsection (9), paragraphs a) and b), Mpt. 77/A. §, subsection (7), paragraphs a) and b), Öpt. 40/C. §, subsection (7), paragraphs a) and b), Gov. Decree 4. §, subsection (1), paragraphs a) and b)

b) contains the descriptions and models needed for reviewing the structure and operating of the system, the data transfer rules, the description of interface connections, the user and administrator manuals, the syntax rules and storage structure of data (e.g. business and functional specifications, use cases, system design, data model, object model, database specification; however a software-generated documentation that does not contain meaningful and relevant information about the roles and the operating of the documented data structure, object, function, module, program, or other system component cannot be accepted as a system description or model being in compliance with legal requirements);

c) archived by the financial institution along with each version – together with the current and documented source code – in a clearly identifiable and accessible way.

4.3.2. If the financial institution does not perform software development, it needs to ensure for custom-made or customized software products the following:

a) the software developer hands over the detailed database specification containing the data syntax rules and the data storage structure, as well as the specifications of the software's output and input data and the data transfers between components upon delivery of the software;

b) the institution may access (e.g. through an escrow) the source code files (which should be presented in a documented format, suitable either to be fully compiled or to be executed without compilation, clearly identified, and current) and development documentation, and the process specifications that enable the creation of executable code – in case the service provider fails to perform bug fixes or application development for any reason.

4.3.3. The institution ensures that the source code and the system description of its outsourced system are available at all times, ensuring that recovery point and recovery time objectives are being met, in a suitable format for further use.

4.4. Testing and change management

4.4.1. Pertinent legal provisions: *The institution shall operate an information system which enables the secure separation of the production environment from the development and testing environment, as well as continuous change management and tracking*[22]*. The change management processes of the production system shall guarantee that changes in the system parameters and in the software or code can only be performed in a tested and documented manner*[23]*.*

4.4.2. MNB expects the financial institution, as data controller, to ensure that it manages data according to purpose limitation at all times. The purpose of development and testing are not identical with the purpose for recording the customer data and financial sector secrets, therefore MNB expects the institution to ensure that the integrity, confidentiality and availability of the data it processes is maintained at all times. This means that during processing data for different purposes it is not sufficient to ensure the separation of environments based on integrity and availability, the data should be stripped of the characteristics which justify their classification as secret. Special emphasis should be placed on rendering customer data or financial sector secrets unrecognizable in any environment which runs separately from the production environment (such as testing or development).

[22] Bszt. 12. §, subsection (7), paragraph d), Mpt. 77/A. §, subsection (6), paragraph d), Öpt. 40/C. §, subsection (6), paragraph d), Gov. Decree.3. §, subsection (3), paragraph d)

[23] Gov. Decree 5/B. §, paragraph c)

4.4.3. The institution regulates the go-live and change management procedures for development, the documentation and approval rules, along with the rollback procedures, within its information security management system.

4.4.4. The institution performs development and testing in environments separate from the production environment.

4.4.5. The institution either does not use data from a production systems in the development and test environments or does so only after having anonymised them completely. During the testing or debugging procedure performed directly before go-live, live data can only be processed in the test environment if the controls of the test environment are identical or stricter than the controls of the production systems, and the go-live or debugging test environment is established individually, based on a fully documented procedure, approved by management, for a specified time interval and user base, and live data is immediately deleted from the test environment after the test procedure.

4.4.6. The go-live of executable code is performed by a function which is independent of the developer, and this function also ensures that the source and executable code is identified and stored, the differences between versions are documented, and the version which is approved for go-live and the actual deployed version are identical.

4.4.7. The institution determines the method of restoring the previous executable code or previous operation and the period it requires to be able to do so.

4.4.8. The institution shall ensure that the IT systems, system components and parameters subject to change are tested in a documented manner with reasonable care before go-live. The institution performs functional and non-functional tests, including security tests.

4.4.9. The institution shall ensure the separation of the development and test environment at both database and network level.

4.4.10. The institution shall ensure that the settings of the default passwords and security parameters of purchased or developed IT system components are changed at the time of go-live.

4.5. Outsourcing, subcontracted activities[24]

4.5.1. The institution is responsible for the outsourced or subcontracted activity in the same manner as if the activity was carried out by itself, therefore it is important for the institution to incorporate appropriate contractual guarantees into its contracts to enforce data protection and information security principles and control appropriately that the contract is performed in conformity with these requirements. In connection with data access by third parties, the institution ensures by treating the activity as outsourcing that the service is performed in a transparent manner that enables audits by either the institution or MNB. By subcontracted activity we mean a service which is not carried out by the institution itself, but by a third party provider, and does not qualify as outsourced activity based on relevant legislative background.

4.5.2. During the outsourced or subcontracted managing, processing or storage of data, the institution ensures adequate administrative controls for all subcontractors, agents, suppliers, and persons who may access customer data or financial sector secrets in order to ensure enforceability of confidentiality, integrity and availability standards.

[24] In case of institutions under the remit of the MNB recommendation on the usage of outsourced activities, these requirements also apply to activities performed based on intermediary agreements and other agreements with external service providers.

4.5.3. The institution ensures adequate guarantee arrangements pertaining to outsourced or subcontracted managing, processing or storage of data that customer data or financial sector secrets are managed by the controller only to the degree and for the time necessary to achieve the purpose of managing the data. Furthermore, the managing of data shall be regulated based on the purpose limitation principle.

4.5.4. In case of outsourcing or subcontracting the institution ensures that adequate information is provided to stakeholders so that the entire process of data handling or data processing – including customer data or financial sector secrets – is transparent and auditable by them.

4.5.5. The institution and service provider performing the outsourced or subcontracted activity stipulate in their contract:

a) the minimum set of regulations to be prepared and adhered to by the service provider;

b) the IT security tasks and responsibilities of the service provider, including the task of risk analysis of outsourced or subcontracted activities and its scope;

c) the recovery time objectives (RTO) and recovery point objectives (RPO) expected by the institution;

d) the service provider's obligation to perform the business continuity planning and preparation (even before starting the delivery of the service);

e) the responsibility of the service provider for the applicability of its business continuity procedures;

f) the method and frequency of testing these procedures and the way to be reported to the institution;

g) the procedures and transfers after the terminating the contract (assets, data, data structures, process descriptions, system designs, documentation, source codes, business logic solutions) the format of the transfer, copyright and property rights, licence and royalties, as well as the obligation to cooperate and the definition of the organisation responsible for bearing the costs arising in connection with these obligations.

4.5.6. The institution considers compliance with the outsourcing requirements in all activities where a third party can access customer data or data suitable to identify or authenticate the customer directly or indirectly, in any way, regardless of its role and legal justification.

IV. OPERATIONS

5. ADMINISTRATIVE PROTECTION

5.1. Procedures of operations

5.1.1. Pertinent legal provisions: *the institution shall have processes and procedures regulating the operation of its information systems.*[25] *The processes for the operation of production information systems are regulated, documented, and reviewed with a regularity which corresponds to the relevant internal rules;*[26] *maintenance of the production system is regulated and is consistent with availability*

[25] Bszt. 12. §, subsection (7), paragraph a), Mpt. 77/A. §, subsection (6), paragraph a), Öpt. 40/C. §, subsection (6), paragraph a), Gov. Decree 3. §, subsection (3), paragraph a)
[26] Gov. Decree 5/B. §, paragraph b)

requirements[27]; the production system and operation processes ensure the integrity of system elements and the processed information[28]; the production system and operation processes ensure the adequate protection of the system and communication[29]. The rules and procedures guarantee that the system's security level, the application of updates and operation of software are maintained at all times[30].

5.1.2. The infrastructure level operational procedures and documentation provide the necessary professional support to keep the protection of information systems updated, to ensure its daily operation, for the tasks concerning the operation and business continuity of the system, and for an effective recovery following a disaster. The institution supports the execution of the aforementioned tasks by fulfilling the following requirements.

5.1.3. The institution regulates the preparation, documentation, and review of its operational rules, technical and administrative documents and records (henceforth: operational procedures) in its information security management system.

5.1.4. MNB expects operational procedures to enable a trained professional to operate or ensure the recovery of the system, even if the original operator or service provider is no longer available.

5.1.5. Operational procedures ensure that an independent IT audit can ascertain the adequacy of tasks defined by the institution and whether the institution executes these tasks in a satisfactory manner.

5.1.6. The institution prepares at least the following operational procedures during the introduction of the system into the production environment, and reviews and updates them if changes in the system occur, but at least during the review of the risk assessment:

a) the description of production environments for each system (operational architecture, operating environments, database management system, monitoring solutions)

b) the operating manuals of the system: regular activities for operations and monitoring to be undertaken, log review tasks, reports and records generated during the execution of these tasks, responsibilities concerning record keeping.

5.1.7. The institution ensures that the operational procedures are stored – under adequate physical and logical protection – on the backup location (i.e. a different location from the headquarters or primary location of operations).

5.1.8. The institution considers and, in a risk-proportionate manner, decides whether it prepares the settings and installation manuals for its individual systems and the manner it introduces these manuals into its information security management system.

5.2. Inventory of software assets

5.2.1. Pertinent legal provisions: *the institution shall, at all times, maintain a complete and up-to-date inventory of its business software assets.*[31]

5.2.2. The institution determines the type and version of software it allows to be installed on a particular device and ensures that only the explicitly allowed software are actually installed.

---

[27] Gov. Decree 5/B. §, paragraph m)
[28] Gov. Decree 5/B. §, paragraph o)
[29] Gov. Decree 5/B. §, paragraph p)
[30] Gov. Decree 5/A. §, subsection (3), paragraph c), subparagraph cd)
[31] Bszt.12. §, subsection (9), paragraph g), Mpt. 77/A. §, subsection (7), paragraph g), Öpt. 40/C. §, subsection (7), paragraph g), Gov. Decree 4. §, subsection (1), paragraph g)

5.2.3. The institution ensures that the up-to-date inventory of all its business software assets (at least the baseline software, application systems, database management software) can immediately be produced from its information systems or, failing that, it maintains a comprehensive and up-to-date inventory manually.

5.2.4. The software inventory is consistent with the accounting records of the institution and also contains those software assets which have been installed onto devices which cannot be accessed from a given network.

5.2.5. Exemplary practice

The institution considers, and, in a risk-proportionate manner, decides whether it introduces an independent software asset inventory and whether it regularly checks the content of the inventory against the software actually installed on its devices.

5.3. Agreements proving the legitimacy of installed software

5.3.1. Pertinent legal provisions: *the agreements that prove the legitimate use of the software shall be available at the institution at all times.*[32]

5.3.2. The institution obtains and keeps proof of the legitimate use of its software assets – contracts, licence invoices, declarations of licences – and stores them in a manner that ensures that an internal or external licence audit can be conducted at any point in time.

5.3.3. The institution checks regularly whether the installed software on its devices – and the main version of the installed software – are consistent with its licence agreements.

5.4. Identification of information system components

5.4.1. Pertinent legal provisions: *the institution shall ensure, based on the evaluation of the results of its security risk assessment, in a risk-proportionate manner, that the most important components of the system (devices, processes, individuals) are identifiable in a clear and retraceable way.*[33] *The institution ensures that the components of its production system are identifiable and documented.*[34]

5.4.2. The institution maintains a technical inventory of the devices it owns or uses – e.g. hardware and software assets, personal authentication devices necessary for its information technology and data communication operations – which records at least the following:

a) exact description of the asset, its model, unique identifier,
b) the actual and exact location of the asset – its physical location, or, for mobile devices, the name of the user,
c) the hardware and software configuration of the device,
d) the owner, user of the asset, or the person responsible for it.

5.4.3. The inventory is up to date at all times, consistent with the accounting records, and contains the assets of the institution that cannot be accessed from a given network segment.

---

[32] Bszt. 12. §, subsection (9), paragraph f), Mpt. 77/A. §, subsection (7), paragraph f), Öpt. 40/C. §, subsection (7), paragraph f), Gov. Decree 4. §, subsection (1), paragraph f)
[33] Bszt. 12. §, subsection (6), paragraph a), Mpt. 77/A. §, subsection (5), paragraph a), Öpt. 40/C. §, subsection (5), paragraph a), Gov. Decree 3. §, subsection (2), paragraph a)
[34] Gov. Decree 5/B. §, paragraph a)

5.4.4. The institution identifies the individuals who are authorised to enter its critical locations of operation and records every entry to the premises.

6. PHYSICAL PROTECTION

6.1. Pertinent legal provisions

The institution creates and continuously operates its information technology control system that monitors the secure operation of the information systems[35], and provides an environment with adequate physical security for its production systems.[36]

6.2. General requirements

To ensure business continuity and the confidentiality, integrity and availability of data, MNB expects the institution – in addition to administrative and logical security –to ensure physical access controls for its critical infrastructure components, to ensure auditability of access, and to continuously monitor deviations of the operational environment, and to correct and rectify their effects. For this effect, the institution ensures that at least the following controls are in place:

6.2.1. The institution, through organisational, procedural, physical, and technological controls, ensures that rooms or containers where critical infrastructure components (networking devices, servers, systems, and information security solutions) are concentrated can only be accessed by authorised personnel in a controlled and logged manner (e.g. access control system, adequate wall material, grating).

6.2.2. The institution monitors and checks the environmental parameters of the rooms containing critical infrastructure components and ensures that the pre-defined individuals are immediately alerted, at least in the cases when any the following parameters reach an unacceptable level:

a) power supply (disruption, fluctuations, outage),
b) temperature too high or too low,
c) humidity,
d) fire, smoke,
e) moisture, water,
f) unexpected opening of doors/windows and keeping them open,
g) unexpected movement of personnel.

6.2.3. The institution creates and maintains risk-proportionate controls to prevent events related to environmental parameters – as set out in point 6.2.2 – which may impair the safe state of running (including but not limited to fire-prevention measures and controls preventing unauthorised access).

6.2.4. The institution considers in its risk assessment whether the use of wall materials, doors and windows which may hinder the spread of a fire is warranted.

6.2.5. The institution ensures that power supply is uninterrupted during both shorter and longer outages.

6.2.6. The institution ensures that the operational temperature remains within a safe range.

---

[35] Bszt. 12. §, subsection (5), Mpt. 77/A. §, subsection (4), Öpt. 40/C. §, subsection (4), Gov. Decree 3. §, subsection (1)
[36] Gov. Decree 5/B. §, paragraph q)

6.2.7. The institution ensures that physical access control devices undergo regular maintenance and checks regularly whether they are still operable.

6.2.8. Exemplary practice

a) The institution may, in a risk-proportionate manner, ensure, that the physical access control measures of rooms and containers where critical infrastructure components are concentrated, are complemented with a video recording system in a manner that is compliant with data protection regulations.

b) The institution may, in a risk-proportionate manner, strengthen the fire protection of rooms and containers where critical infrastructure components are concentrated with an automatic fire suppression system.

7. NETWORK PROTECTION

7.1. Pertinent legal provisions

The financial institution shall, based on the evaluation of the results obtained during its security risk assessment, ensure the confidentiality, integrity, and authenticity of data in transit.[37] *The institution shall ensure that the data communication and system connections of the production system are documented and controlled in order to ensure the confidentiality, integrity, and authenticity of data communication;*[38] *the organisation detects and handles security events.*[39] *Each external interface of the system shall be regulated and controlled.*[40]

7.2. General requirements

The documentation of data communication, system connection and network should enable the traceability of data flows of business processes and the identification of the connections (interfaces) and devices which support the processes. The control measures required by the data classification should be applied to devices and connections that have been identified in such a manner, ensuring that transmitted data remains authentic and retains its confidentiality and integrity within the communication medium.

7.3. Documentation of data communication systems

7.3.1. The institution ensures that the operational procedures of data communication, system connections, and network management are prepared and maintained, based on the requirements of its information security management system.

7.3.2. The institution ensures that the documentation on the data communication enables the infrastructural traceability of each business process at data connection and network level. In order to achieve this, the institution should at least have the following documents ready:

a) a data connection chart that contains the devices, systems, and system components; along with the identifier, types and characteristics of the connections among them,

---

[37] Bszt. 12. §, subsection (6), paragraph e), Mpt. 77/A. §, subsection (5), paragraph e), Öpt. 40/C. §, subsection (5), paragraph e), Gov. Decree 3. §, subsection (2), paragraph e)
[38] Gov. Decree 5/B. §, paragraph j)
[39] Gov. Decree 5/B. §, paragraph r)
[40] Gov. Decree 5/A. §, subsection (3), paragraph c), subparagraph cc)

b) a chart of network topology which can be mapped to the data connection chart,

c) data centre layout,

d) the description of network zones and access rules.

7.4. Protection of data in transit

7.4.1. The institution transmits data which enables the identification or authentication of users or customers or constitutes a financial sector secret only in an enciphered form on a remote access network, including private networks based on leased lines.

7.4.2. The institution transmits passwords or other authentication data over both remote and local area networks in encrypted format only.

7.4.3. The institution regards wireless networks, data transfer methods and devices using such methods (e.g. WiFi, Bluetooth, mobile communication devices) which may be used to transmit client data or data which may constitute sector secret, or which are connected to the institution's network, as critical risk elements.

7.4.4. The institution, to secure authorised remote access or connections via mobile devices, takes at least the following actions:

a) The institution grants access to its systems within its internal network (which encompasses virtual private networks and e-mail systems) to authorised users and devices only, through a centrally managed solution, only to the necessary extent and to the necessary devices.

b) The institution requires and through technological means enforces at least the following security settings on the devices: encryption, automatic screen lock, a PIN code of at least 5 digits to unlock the screen or a more secure solution, data loss prevention, two factor authentication, limited data access, remote wipe.

c) The institution, observing security considerations, defines and enforces the minimum model or version number (at least for hardware, operating system, and relevant applications) that is required for the connection. The institution prohibits administrative access to devices used for connection and cracked devices (rooted, jailbroken) from being used for connection.

d) For virtual private networks, the institution uses encryption and integrity algorithms, authentication methods and protocols, along with technological security validation (including but not limited to the checking the adequacy of malware protection, adequacy of installed security updates, use of local firewall, whether split tunnelling is disabled, whether storage encryption is enabled, or the existence of data loss prevention solutions).

e) The institution completely prohibits users' own devices (BYOD) to connect to its IT infrastructure, or allows connections only if the devices are reinforced with the necessary controls in a risk-appropriate manner, with at least the requirements defined in points a), b) and c) being enforced.

f) The institution ensures the continuous monitoring of remote connections and the – preferably automated – detection and management of security events.

g) The institution ensures the regular review and update of its remote access rules, settings, and authorised users.

h) The institution ensures the fault tolerance, availability, backup of configuration, logging of important events, and central log collection and analysis regarding the devices managing remote connections.

7.4.5. The institution ensures the confidentiality, integrity, and authenticity of data during network transmission, and the auditability of the fulfilment of these criteria.

7.5. Network perimeter protection

7.5.1. MNB expects that network connections – including data flow between network segments – are designed in a manner that only traffic which is required for business needs and is explicitly permitted is allowed to pass through.

7.5.2. The institution creates and maintains a set of network connection rules, which are adequately regulated, justified by business needs, authorised, documented, identifiable, and regularly (at least during the risk assessment) updated.

7.5.3. The institution enforces the permitted communication and connection rules through technological means using network perimeter protection solutions for each network layer in a risk-proportionate manner (e.g. firewall, intrusion prevention system, application level firewall, web and e-mail content filtering, data loss prevention system), and provides a risk-proportionate defence against external attacks. If the network perimeter protection solution becomes overloaded or fails, the institution closes the connection. For the perimeter of its network environment accessible through the Internet, the institution also uses risk appropriate higher-level network (application) layer solutions to monitor network traffic, to filter inappropriate content, and to protect its web applications. For external connections, encrypted traffic is also inspected.

7.5.4. The institution ensures the automated filtering of unwanted network connections and events.

7.5.5. The institution ensures data loss prevention in a risk-appropriate manner. In this regard, the institution ensures at least the following:

a) within its information security management system, the institution details the operational tasks and responsibilities concerning data leaks, with special regard to the management of administrator access and data leakage incidents;

b) the institution conducts network discovery regularly, but during the update of its risk assessment at the latest, to identify the locations where sensitive data are stored;

c) to control potential data leakage channels, the institution deploys risk-proportionate protection and monitoring solutions for, at least, the following: web access, e-mail connections, endpoints, mobile devices, file servers, cloud services and printers;

d) the institution prohibits the use of external storage devices completely for its users, or allows their limited use under adequate controls only – e.g. privileged rights, content control, data loss prevention solution etc.;

e) the institution prohibits access to Internet content carrying data leakage and malware risk, and, in a risk-proportionate manner, filters traffic through technological means – at least covering webmail, online storage, and peer-to-peer solutions. In order to filter content which may pose a risk, the institution uses dynamically updated URL lists;

f) the institution, in order to manage data leakage risks, operates a comprehensive data loss prevention (DLP) solution – which supports the processes preventing data leaks and

monitoring potential data leak channels in a centralised manner – proportionately to security risks.

7.5.6. The institution assesses and manages risks concerning its network perimeter protection and the security of its solutions which transmit voice and multimedia over network (VoIP, SIP).

7.5.7. The institution ensures

a) the regular review of rules, regulations, perimeter protection devices and software, and their regular planned update,

b) the automated update of attack patterns, sources, and URL lists.

7.5.8. The institution ensures a risk-proportionate and multi-layered protection against denial of service attacks on its external internet connection at bandwidth, connection and application level, which would potentially result in the failure or slowing down of its services, servers, network devices.

7.5.9. The institution, in order to protect its devices accessible from the internet – e.g. communication servers and web servers – ensures that webservers are placed within a demilitarised zone (DMZ), whereas web services, financial applications and databases are located in the protected networks behind the DMZ.

7.6. Security event management

7.6.1. The institution ensures that discovered security events (incidents) are managed in a documented manner and the lessons learnt are subject to feedback.

7.6.2. The institution maintains a register of the incidents which affect the proper operating of its information systems or information system components, and their resolutions.

7.6.3. The institution ensures the continuous monitoring of its protection system to detect and manage attacks as soon as possible – preferably in an automated manner.

7.6.4. The institution creates a documented incident management process which includes at least the following:

a) roles, tasks, processes of communicating and contacting authorities, supervisors, directly affected clients in case of a perceived or actual attack or damage,

b) detailed, practice-oriented procedures for managing known incidents (e.g. monitoring system alerts, DDoS attacks etc.),

c) processes that ensure the testing of the adequacy of the incident management.

7.6.5. The institution reviews the adequacy of its incident management processes during the review of its risk assessment at the latest.

7.7. Protection against viruses and other malware

7.7.1. Pertinent legal provisions: *based on the evaluation of the results of its security risk assessment, the institution shall protect its system against viruses and other malware.*[41] *The institution ensures the antivirus and antimalware protection of its live production system.*[42]

[41] Bszt. 12. §, subsection (6), paragraph g), Mpt. 77/A. §, subsection (5), paragraph g), Öpt. 40/C. §, subsection (5), paragraph g), Gov. Decree 3. §, subsection (2), paragraph g)

[42] Gov. Decree 5/B. §, paragraph i)

7.7.2. The institution runs software which enables the detection of viruses and other malware, and ensures that the software, the databases and signatures are up-to-date and logged.

7.7.3. The institution ensures that automated update of its antivirus and antimalware system, and that full scans are performed on a regular – at least weekly – basis. Full scans may be replaced by other, adequate controls.

7.7.4. The institution ensures that the settings of the antivirus and antimalware system may only be modified according to the criteria and procedures set out in its information security management system.

7.7.5. The institution ensures that files which had been identified as threats can only be transferred to end users following an adequate professional review and the elimination of potential danger.

7.7.6. The institution ensures controls against malicious code even in encrypted connections related to Internet access or e-mail.

7.7.7. The institution ensures that its information systems only run software with ongoing product support and security updates. The institution ensures the regular testing and installation of updates to its live systems to mitigate the risk of malware deployment using known software vulnerabilities.

7.7.8. The institution maintains multi-layered, defence-in-depth measures and operates an endpoint security software with a central management interface.

7.8. E-mail protection

7.8.1. The institution defines the security processes and rules of using e-mail within its information security management system.

7.8.2. The institution provides multi-layered (central and endpoint) and multi-functional (against spam, e-mail containing malicious code or malicious links, phishing, e-mails indicating data leaks etc.) to ensure its e-mail security. In this regard the institution ensures that every e-mail – even those that are encrypted or contain an encrypted attachment – is checked by its central e-mail protection solution and filtered if necessary.

7.8.3. The institution allows the use of e-mail for devices, network segments and people only if justified by business needs or technical reasons.

7.8.4. The institution enables sending and receiving e-mails through encrypted channels, and based on the content of the e-mail, provides the means of encrypting attachments in a risk-proportionate manner.

7.8.5. The institution maintains appropriate settings in its e-mail system and prevents the propagation or forwarding of e-mails from unverified sources. The institution maintains the proper Domain Name System (DNS) settings of its e-mail system.

7.8.6. The institution quarantines unwanted or potentially risky e-mails in a risk-proportionate manner. Th institution ensures that e-mails which had been identified as a threat cannot be forwarded to end users without adequate professional review and filtering.

7.8.7. The institution ensures that the rules, settings, signatures of the protection system are regularly reviewed and updated.

7.8.8. The institution ensures the continuous monitoring, fault tolerance, availability of the protection system, backup of its configuration, logging of its pertinent and security events, central log collection, log analysis, and automated alerts if necessary.

8. LOGICAL PROTECTION

8.1. Common requirements of logical protection

8.1.1. Pertinent legal provisions: *based on the evaluation of the results of its security risk assessment, the institution shall possess at least the following: […] inspections and procedures ensuring the self-defence of the IT security system, as well the integrity and comprehensiveness of the protection of its critical elements.*[43] *All the software together shall be suitable for logical protection commensurate with the level of security risks, and the protection of integrity.*[44]

8.2. Database security

8.2.1. The institution defines the rules and procedures for the protection and operating of databases within its information security management system.

8.2.2. The institution prohibits direct database access. Exceptional cases are authorised on an individual basis, and the institution pays special attention to the management, oversight, and appropriate logging of activities during the direct modification of databases or records found therein. This process is regulated within the information security management system of the institution, and the institution ensures that these activities are continuously monitored by an independent person or organisation.

8.2.3. The institution reviews the security settings of its database management systems regularly, based on vendor and professional recommendations, and defines and enforces the hardening requirements of database configuration and security parameters in a risk-proportionate manner, including database security parameters, user and password requirements, logging and auditing settings.

8.2.4. The institution ensures the continuous monitoring of the databases' operation, along with the – preferably automated – detection and management of events.

8.2.5. The institution ensures that its database systems are fault tolerant, ensures their availability, prepares backups of configuration settings and databases, and ensures the logging, centralised log collection, and analysis of important events in a risk-proportionate manner.

8.2.6. The institution uses database encryption in a risk-proportionate manner and ensures the secure management of encryption keys.

8.3. Security of virtual environments

8.3.1. The institution defines the rules and procedures for the protection and operating of virtual environments within its information security management system.

8.3.2. The institution reviews the security settings of its virtual environments, based on vendor and professional recommendations, and defines and enforces the hardening requirements of database configuration and security parameters in a risk-proportionate manner. The institution ensures that updates are applied regularly to its virtual environments.

8.3.3. The institution ensures the continuous monitoring of the operation of its virtual environments' components, along with the – preferably automated – detection and management of events.

---

[43] Bszt 12. §, subsection (6), paragraph b), Mpt. 77/A. §, subsection (5), paragraph b), Öpt. 40/C. §, subsection (5), paragraph b), Gov. Decree 3. §, subsection (2), paragraph d)

[44] Bszt. 12. §, subsection (10), paragraph f), Mpt. 77/A. §, subsection (8), paragraph c), Öpt. 40/C. §, subsection (8), paragraph c), Gov. Decree 4. §, subsection (2), paragraph e)

8.3.4. The institution ensures that its virtual systems are fault tolerant, ensures their availability, prepares backups of configuration settings and virtual devices, and ensures the logging, centralised log collection, and analysis of important events affecting system components in a risk-proportionate manner. The institution creates and updates the files which are necessary for the deployment of virtual environments in a manner which is proportionate to security risks.

8.3.5. The institution ensures the encryption of virtual devices (virtual guests, discs), and the management of encryption keys in a risk-proportionate manner.

8.4. Data transfer

8.4.1. The institution ensures that data transfers among its systems, system components are conducted in an automated manner, via standardised interfaces. The institution prohibits manual or file-based data transfers, and creates a timeline for replacing such existing solutions. The institution maintains the confidentiality, integrity and availability of data during the replacement phase.

8.4.2. The institution ensures that the IT integrity requirements are met at all times by its systems which are involved in making business decisions, reports, and processing customer data. In such procedures the institution prohibits data creation by end users through office software suites, high level developer tools or other means, except when it is mandated by legislation or proceedings instituted by a public authority, in which case the institution ensures through compensating controls that basic integrity requirements are fulfilled.

9. RULES OF ACCESS

9.1. Pertinent legal provisions

Access by end-users to the live operational system shall be controlled both at application and infrastructure level, documented and tested at a frequency determined in the relating regulations[45]*. The institution shall have a description of the rules of access to data available at all times,*[46] *and it shall ensure that the protection offered by access controls of backup copies is equivalent to the source system.*[47] *The general users (people and program entities) and privileged users (authorised with special rights) – system administrators in particular – can have access to the information to be protected and to the elements of the system processing such information, and initiate activities, based on their strictly defined respective roles, and only pre-defined privileged users can be allowed to grant other users access in accordance with their respective roles and in a controlled manner.*[48]

9.2. Regulation of access

9.2.1. The institution, based on the principle of least privilege, defines and documents the rules governing access of IT and business roles. The institution, during this process, defines and documents the roles that would violate the separation of duties principle.

9.2.2. The institution defines the rules of access within its information security management system.

---

[45] Gov. Decree 5/B. §, paragraph e)
[46] Bszt. 12. §, subsection (9), paragraph d), Mpt. 77/A. §, subsection (7), paragraph d), Öpt. 40/C. §, subsection (7), paragraph d), Gov. Decree 4. §, subsection (1), paragraph d)
[47] Bszt. 12. §, subsection (8), Mpt. 77/A. §, subsection (6), paragraph e), Öpt. 40/C. §, subsection (6), paragraph e), Gov. Decree 3. §, subsection (4)
[48] Gov. Decree 5/A. §, subsection (3), paragraph c), subparagraph ca)

9.2.3. The institution enforces the rules of access within its information system through technological means, including the rules prohibiting the simultaneous use of roles which would result in a violation of separation duties.

9.3. Rules of access to data

9.3.1. The rules of access define system variables and configuration values that determine that data can be accessed by authorised users, allowing operations only that are strictly necessary for their role. The rules of access are defined in the technical documentation of each system or in a separate document.

9.3.2. The institution defines its rules of access to data within its information security management system.

9.3.3. As part of access management, the institution identifies authorisation objects and resources which may be accessed by users (accounts) defined within the information system, which users represent processes (e.g. processes, stored procedures, automated activities), or people (e.g. employees, suppliers, partners, customers).

9.3.4. The institution evaluates and groups the authorisation objects and resources based on risk. The institution defines the method and rules of user (account) access for each group.

9.3.5. The institution maintains an inventory on correlations between authorisation objects and resources, users (accounts) and representing entities at all times.

9.3.6. The institution, during the management of access, continuously monitor the planned and implemented correlations, and the enabled access, and ensures that their consistency is reviewed regularly.

9.3.7. The institution, for each system, defines at least the following within its information security management system:

a) system identifier (network ID), network connections, data connections, ports and protocols, method of user authentication;

b) system level security settings;

c) local and remote users, user groups, default user accounts, account settings, content of local policy and security policy (e.g. password policy, log settings etc.)

d) for directory systems users, user groups, default user accounts, account settings, access control lists, organisational units, published (shared) resources, access rights to directory objects, domain security settings (e.g. password policy, log settings)

e) access rights to resources, access control lists, resource event log settings,

f) shared folders, parameters of sharing, rights to share resources and files,

g) user management within applications, connecting user groups (roles) and business activities, the process for managing general security settings (e.g. password rules, log settings, technical users for data connections),

h) for database management systems, in addition to the previous requirements, account settings, system and object privileges for non-default roles, profiles, and security settings (e.g. password rules, log settings),

i) rules for managing and maintaining an inventory of privileged users (e.g. system administrator accounts) and technical users and the people responsible for each;

j) the list of user accounts for which the institution finds it necessary to ensure emergency access.

9.3.8. The institution regularly reviews and updates the security settings of the systems based on the professional hardening guidelines and the manuals provided by the vendor.

9.4. User administration

9.4.1. Pertinent legal provisions: *the access rights of users shall form a uniform, closed system which ensures the realisation of business processes, furthermore the activities of users shall be logged, and automated warnings shall be generated upon the occurrence of critical, extraordinary events;*[49] *privileged access to production environments shall be regulated, documented and reviewed regularly, furthermore activities of privileged access shall be logged, the integrity of log files shall be ensured, and automated warnings shall be generated upon the occurrence of critical, extraordinary events;*[50] *remote access to production environment is regulated, documented and reviewed as set out by relevant internal procedures.*[51] *The institution shall ensure, based on the assessment of the results of its security risk assessment, in a risk-proportionate manner, the operation of a regulated, documented and regularly reviewed user administration (access levels, individual access rights, authorisation, responsibilities, logging of access, extraordinary events).*[52]

9.4.2. The institution requires that access to its information system is bound to individual user accounts which are unambiguously connected to a natural person, and the systems' usage is regulated within its information security management system.

9.4.3. The institution ensures that the creation, deletion (disabling), and modification of user accounts is conducted in an authorised and documented manner as defined in its user access procedure.

9.4.4. The institution ensures that during the creation and forwarding of user accounts, only the person can obtain the credentials for whom they have been intended, and ensures the unambiguous connection between the user account and the natural person responsible for its use, through either the information system itself or a separate register.

9.4.5. The institution ensures that within the information systems, only authorised users are granted access, and this can be ascertained at any point in time.

9.4.6. The institution defines the password complexity and expiration rules in each system in a manner proportionate to the risks of the activities the user is authorised to conduct, in a manner which is on par with the users' capabilities.

9.4.7. The institution considers the asset to be protected, the potential risks and the necessary expenses while defining the requirements for user identification and passwords, procedures and tools of information systems containing customer data or financial sector secrets.

9.4.8. The institution logs data of user account logins and logouts, password changes and other, authentication-related events, with the specific exception of the password which must not be logged, no matter whether the system in question is critical or non-critical.

9.4.9. The institution uses at least one additional authentication factor besides user account – e.g. dynamic code or certificate – when authenticating remote access.

---

[49] Gov. Decree 5/B. §, paragraph f)
[50] Gov. Decree 5/B. §, paragraph g)
[51] Gov. Decree 5/B. §, paragraph h)
[52] Bszt.12. §, subsection (6), paragraph c), Mpt. 77/A. §, subsection (5), paragraph c), Öpt. 40/C. §, subsection (5), paragraph c), Gov. Decree 3. §, subsection (2), paragraph c)

9.4.10. The institution sets out the methods of emergency access within its user access procedures, maintains a unified register of user accounts enabled for emergencies, and reviews the compliance of emergency access regularly.

9.4.11. The institution ensures that the rules for storing and using credentials of technical users are defined within its information security management system and enforced, incorporating the “least privilege” and “four eyes” principles, as a minimum.

9.4.12. The institution ensures that at least the following rules are enforced in a risk-proportionate manner within its information systems:

a) the password should consist of as many characters (at least 12 for end users, 15 for technical or administrative accounts) or passphrases as possible,

b) the password should not be dictionary based,

c) the password should be hard to guess (should not contain reference to the user, their relatives, their property),

d) the last 5 passwords should not be reused,

e) the expiration period should be set between 1 and 90 days,

f) the account should be locked after 5 consecutive unsuccessful logon attempts,

g) the period of lockouts (time-out periods) increase after further unsuccessful logon attempts,

h) user IDs of system administrators, application administrators and other users who may use several roles to access a system should be separated for each role (e.g. the user and administrative account should be differentiated),

i) passwords are stored only in an encrypted format, except properly secured technical passwords for emergency access,

j) the requirement to change the initial password is enforced within the information system.

9.5. Review of administrative rules of access and users

9.5.1. The institution ascertains through a documented review that the access and user administrative rules are being adhered to, based on the procedures in its information security management system, with the regularity defined therein, but at least annually.

9.6. Encryption, key management, certificate management

9.6.1. The institution defines the rules and procedures of the applied encryption, key management, and certificate management within its information security management system.

9.6.2. The institution uses only open, standardised cryptographic methods and algorithms in its information systems.

9.6.3. The institution determines cryptographic key length based on the planned key expiration and the characteristics of the applied algorithms (e.g. symmetric).

9.6.4. The institution continuously monitors available technological solutions and the simplification of deciphering. The institution retires outdated solutions, considering the security of already protected information.

9.6.5. The institution creates and maintains a documented, comprehensive, standardised procedure for managing cryptographic keys, which contains at least the following:

a) secure key generation and distribution,
b) secure key storage, management of storage of authentication and encryption keys,
c) regular key renewal; the revocation, renewal, destruction of compromised or expired keys,
d) method of key sharing and dual access,
e) archiving of encrypted files and their keys, considering the advancements of technology.

9.6.6. The institution ensures that secret keys are not exported, and in exceptional cases, the export takes place on an individual basis, in a controlled and encrypted manner.

9.6.7. The institution creates a central register for its self-signed and externally signed certificates and certificate storing devices. The institution ensures that the register is up to date at all times.

9.6.8. The institution defines and ensures that the contact persons whose contact information have been forwarded to the external service provider have substitutes.

9.6.9. The institution ensures the hardening and information security review of its public key infrastructure (PKI), and during its architectural design phase ensures the proper protection of the Certificate Authority (CA) servers and their keys, furthermore, ensures the proper separation of virtualised solutions.

9.6.10. The institution ensures the backup of keys and servers of PKI in a manner that is protected against being compromised.

9.6.11. The institution ensures that the applied settings for CA servers and certificates issued by these follow the reasonably expected best practices concerning algorithms, key lengths, certificate templates, operational functions, expiration dates, certificate storage and sharing methods, publication and validity of certificate revocation lists.

9.6.12. The institution ensures the continuous monitoring of its PKI system, and the – preferably automated – detection and management of events.

9.6.13. The institution ensures the fault tolerance, availability, backup of configuration and keys, the logging of important events, the central collection and analysis of logs, and ensures that – security and functional – vendor updates are applied regularly to its PKI environments.

10. BACKUP, ARCHIVING, RECOVERY, STORAGE MEDIA MANAGEMENT

10.1. Pertinent legal provisions

The institution shall possess such backups, backup procedures, and recovery plan pertaining to its information system, which enable the recovery of the system within the timeframe set out in the recovery time objective of the service supported by the system; furthermore the institution shall store backups separately – to avoid their being subject to the same risks – in a fireproof manner, and the institution shall ensure access protection of backups at an equivalent level to the source system.[53] *The backup and recovery process of production system shall ensure a reliable recovery, and recovery from backup shall be tested with the regularity set out in the relevant internal rules, in a documented manner.*[54] *The institution shall ensure, based on the assessment of the results of its security risk*

[53] Bszt. 12. §, subsection (7), paragraph e) and subsection (8), Mpt. 77/A. §, subsection (6), paragraph e), Öpt. 40/C. §, subsection (6), paragraph e), Gov. Decree 3. §, subsection (3), paragraph e) and subsection (4)
[54] Gov. Decree 5/B. §, paragraph d)

assessment, in a risk-proportionate manner, the regulated and secure handling of storage media.[55] *The protection of storage media in production systems shall be regulated, access shall be adequately limited, and limitations shall be maintained, among other methods, through regular reviews and audits.*[56]

10.2. General requirements

The objective of creating backups is to ensure that data may be restored within an acceptable time limit (recovery time objective, RTO) and with an acceptable level of data loss (recovery point objective, RPO), while applying proper access rights. MNB expects that as part of archiving data, the institution ensures that data can be restored at a later point in time, therefore the institution should use technologies and solutions that enable this.

10.3. Rules for creating backups and archives

10.3.1. The institution defines the rules and procedures of the creation and testing of backups and archives of data within its information security management system.

10.3.2. The institution defines its backup procedure in a manner that ensures – in accordance with the service continuity requirements of the institution – that the type, frequency and number of copies result in an acceptable risk of outage and data loss.

10.3.3. The institution ensures the following:

a) backups are entered into the inventory;

b) in addition to the creation of backups and archives of data, all other – data and software – components, which are necessary for restoring said data, are also included in a recoverable manner or creates an archive copy thereof;

c) during the selection of backup and archive media, vendor recommendations – e.g. retention time, number of allowed rewrite cycles, storage conditions – are taken into consideration;

d) storage media is handled in accordance with the requirements defined in the classification for the stored data;

e) access controls of backup and archive media provide the same level of security as those in the source system;

f) backup and archive storage media and the devices necessary for restoring said data are available at all times (see point 11.2.7), including a copy at the recovery site;

g) encrypted backup and archive media are protected at all times, even if changes occur in technology.

10.3.4. The institution ensures the fire-proof storage conditions of backup media by storing backup and archive media at multiple locations, on the recovery site, and either in a separate room which is fireproof for at least 30 minutes with appropriate physical access controls, in a different fire section within the same building, or in a different, fire code compliant building separated from the building used for storing and processing production data.

[55] Bszt. 12. §, subsection (6), paragraph f), Mpt. 77/A. §, subsection (5), paragraph f), Öpt. 40/C. § subsection (5), paragraph f), Gov. Decree 3. §, subsection (2), paragraph f)

[56] Gov. Decree 5/B. §, paragraph n)

10.3.5. The institution, within its backup procedures, sets out that at least the following operational procedures are prepared:

a) the general overview of the backup system of the financial institution, which contains:

aa) the comprehensive definition of data which is subject to backup,

ab) the method of backup, definition of backup software and devices, the storage location of backups,

ac) the cases that may result in data loss (e.g. backup for the previous day will not contain the transaction that took place on a given day),

ad) the interval when backups are being conducted (executed),

ae) the retention time for backups,

af) the method of taking backups into inventory,

ag) the procedures for verifying whether backups are still readable, the frequency of verification,

b) backup procedures, meaning procedures for performing backup and verification of successful backups;

c) restore procedures, meaning procedures for restoring individual backups and verification of successful restoration;

d) recovery procedures, meaning the recovery of IT and data communication systems from backups and the verification of a successful recovery.

10.3.6. The institution, based on its backup procedures, conducts regular, documented review of the existence of backups and their suitability for recovery.

10.4. Archiving

10.4.1. Pertinent legal provisions: *the financial institution shall possess a data storage system which enables the retrieval of records as set out by legislation and that archived data will be retained in a searchable and retrievable manner for the retention period as set out by law but at least for five years.*[57]

10.4.2. The institution creates archive copies of its records defined by law, based on its documented backup procedures, and retains the copies for the time period defined by sectoral law – or, lacking a defined retention period, for five years – in a manner that ensures that they can be searched and restored at any time (archive data).

10.4.3. The institution ensures that when replacing its data storage equipment and devices, the archive data are migrated to the new systems, or keeps the old system in operation, or ensures that the old systems' operation can be resumed at any time, in order to restore archive data.

10.5. Storage medium management

10.5.1. Data storage medium is understood as any device or system component that may be used to store data.

[57] Bszt. 12. §, subsection (7), paragraph f), Mpt. 77/A. §, subsection (6), paragraph f), Öpt. 40/C. §, subsection (6), paragraph f), Gov. Decree 3. §, subsection (3), paragraph f)

10.5.2. The institution defines the secure management of storage media, within its information security management system, including a clean desk, and a clean screen policy.

10.5.3. While it is handling the medium, the institution complies with and enforces the physical protection requirements set out for the class of data being stored on the storage medium.

10.5.4. If the data storage medium is retired from service, the institution deletes customer data or data which constitutes sector secret from the storage medium irretrievably, or destroys the storage medium.

10.5.5. The institution maintains an inventory of individual storage media, which contains at least the following:

a) type of storage medium,
b) individual identifier,
c) the natural person responsible for the medium,
d) the location
e) of the storage medium.

10.5.6. The institution ensures the encryption of the data stored on the medium in a risk-proportionate manner, along with the management of encryption keys as set out in point 9.6.

10.6. Data processing of backup and archive data

10.6.1. The institution ensures that storage of data during backup and archival takes place according to the principle of purpose limitation, in line with the provisions of data protection and sectoral regulation. MNB expects that the institution designs its backup procedures in a manner that ensures that customer data and data constituting sector secret are only stored for a period defined by law. Once that period expires, data should be deleted, its connection to the customer should be irrevocably severed.

10.6.2. During the management and storage of backup and archive data the institution should ensure that the requirements set out by storage medium management rules (see point 10.5) are adhered to.

11. SERVICE CONTINUITY

11.1. Pertinent legal provisions

The institution shall, in order to ensure that its activities are conducted and its records are maintained in a secure and up-to-date manner, implement control measures, based on the evaluation of the results of its security risk assessment, in a risk-proportionate manner; the institution shall create and maintain a plan for managing events which may disrupt the continuity of the institution's services (hereafter: service continuity plan).[58] *Furthermore, the institution shall operate an information system for conducting business, along with backup devices, or, in the absence of backup devices, other solutions that ensure the continuity of activities and services.*[59] *Disaster recovery plans shall be tested regularly.*[60]

11.2. Plans for managing events that disrupt service continuity

[58] Bszt. 12. §, subsection (7), paragraph g), Mpt. 77/A. §, subsection (6), paragraph g), Öpt. 40/C. §, subsection (6), paragraph g), Gov. Decree 3. §, subsection (3), paragraph g)
[59] Bszt. 12. §, subsection (7), paragraph c), Mpt. 77/A.§, subsection (6), paragraph c), Öpt. 40/C. §, subsection (6), paragraph c), Gov. Decree 3. §, subsection (3), paragraph c)
[60] Gov. Decree 5/B. §, paragraph k)

11.2.1. MNB expects the service continuity plan to meet the requirements published in general business terms and conditions and announcements.

11.2.2. The institution prepares its service continuity plan within its information security management system, and defines the rules, procedures and operative instructions, and the rules of their verification.

11.2.3. While preparing its service continuity plan, the institution defines its critical business services, identifies the processes which are necessary for conducting business, defines the accepted RTOs and RPOs based on business requirements and data classification (see point 10.2), defines the possible scenarios of process outage, taking at least the credible cases of the following into account:

a) different cases of a partial or complete service outage caused by factors which disrupt workplace use, stemming from natural disasters, from malfunctions caused by human actions, or from IT and data communication infrastructure errors,

b) the unavailability of the production system or the primary processing site,

c) non-conformity, outage, or unavailability of externally performed services,

d) critical cases relevant to the institution, as identified during risk analysis.

11.2.4. The institution defines the following and documents them within its service continuity plans:

a) alternative business continuity procedures to be followed during the unavailability of information technology systems,

b) the detailed operational procedures for switching to backup information technology and data communication systems and for recovery,

c) the operational procedures for returning to normal operation,

d) for each procedure, the designation of people who execute the procedures and the people who are responsible for executing the procedures,

e) the internal roles and responsibilities for each outage case, and the rules of external communication.

11.2.5. During the implementation and review of service continuity procedures, the institution

a) ascertains that the procedures are applicable in practice through a realistic and documented testing process;

b) when testing the service continuity processes, comprehensively documents the important conditions – including each step of the testing process, the required and the measured duration of the test –, the performed actions, and other findings of the successful final test;

c) ensures that all relevant personnel are trained on their procedures, tasks, and responsibilities in a documented manner, and prepares the organisation for the execution of procedures;

d) ascertains in a documented manner – with the inclusion of business organisation units – whether RTOs based on business requirements are achievable and recovery is possible with RPO requirements being met (see point 10.2);

e) if the requirements of point d) have not been successfully achieved, prepares an action plan in order to achieve the desired outcome;

f) documents the result of service continuity testing and ensures that the results are approved by management;

g) following changes in business or service processes, information technology procedures, technology or legislative environment, or following an incident, or, at the latest, during the review of its risk assessment, updates and approves the service continuity plan,

h) stores a copy of its service continuity plan securely in a location other than its headquarters or main location of operation, or at the backup locations, in an up-to-date form.

11.2.6. The institution operates backup devices, or lacking these, other solutions that ensure service continuity. In order to achieve this, the institution

a) ensures that its backup devices are able, automatically or through manual intervention, to maintain at least the full operation of critical business processes during a disruption of production devices within the defined RTO, with an acceptable RPO,

b) operates the backup devices referred to in point a) at a different location than the primary site based on the security risks (see point 11.2.7),

c) maintains a backup processing site that provides adequate equipment for the personnel necessary for critical business processes, in order to ensure service continuity,

d) chooses its backup site and its backup processing site based on the criteria set out in point 11.2.7,

e) utilises solutions equivalent to points a)-d), if the institution chooses not to fulfil the above criteria by itself (e.g. signs a contract to obtain backup location and devices).

11.2.7. Backup site: The institution chooses backup location or backup processing location (henceforth 'backup site') for service continuity purposes, in case its primary location, primary processing location, or the location where the institution operates its production systems becomes unavailable, in a manner that ensures that

a) the backup site is situated in such a distance from the site where the institution operates its production systems that disasters (e.g. fire, earthquake, flooding, unexploded ordnance), traffic events, and other events that may prevent use of or access to the primary site, do not affect the primary and the backup site simultaneously,

b) in order to ensure that requirements set out in point a) are met, existing primary and backup sites should not be closer to each other than 400 metres, newly created backup sites should not be located closer to the primary site than 1000 metres.

c) the sites are equipped with independent power, telecommunication, and data communication access,

d) getting to the backup site and switching operation to the backup site together does not exceed the RTO (see point 10.2)

11.2.8. Exemplary practice

During the preparation of service continuity plans, the institution is advised to consider the following:

a) the service continuity plan should be a scenario-based action plan that enables that procedures are executed in a rapid, error-free manner,

b) creates its service continuity plans in separate documents if necessary (e.g a business continuity plan for backup business processes and a disaster recovery plan for the resumption of operation of the affected information system),

c) if the institution operates a business continuity management system (BCM), ensures that during an outage of the BCM, up-to-date information is available on the backup site.

12. PERSONNEL SECURITY

12.1. Pertinent legal provisions

People who operate or use the production system shall participate in regular information security training, and the institution's labour regulations comply with security requirements.[61]

12.2. Information security training

12.2.1. The institution defines the rules and regulations of information security training within its information security management system.

12.2.2. The institution ensures that users with access to production systems which support its business operations, or to data stored therein, participate in regular, documented information security training – for newly hired employees, within 3 months after their hiring, and at least annually for previously hired employees.

12.2.3. The institution ensures that the people who take part in the operation of its production systems are subject to information security training of high professional standards.

12.2.4. The institution prepares an annual training plan, and ensures that the cost of external training is incorporated in the annual cost plans.

12.2.5. Exemplary practice

The institution, during the annual planning process, may consider security training courses for special subject areas of system administrators and developers, and for systems it plans to implement in the future, in order to ensure that they acquire relevant information.

12.3. Internal labour regulation of personnel security

12.3.1. The institution performs security classification of work roles that require access to business processes directly or indirectly, including external or third party access, based on its data classification. The institution defines the security levels based on the classification for each role and the security requirements for each level within its information security management system.

12.3.2. During the hiring process, the institution checks if the newly hired employee meets the security criteria associated with the security classification of their role.

12.3.3. The institution defines the procedure for changing job positions and the roles of employees (their access to data) within its information security management system.

V. AUDIT

13. INDEPENDENT AUDIT

13.1. The rules of auditing, auditing the security system

[61] Gov. Decree 5/B. §, paragraph s)

13.1.1. Pertinent legal provisions: *taking into account the security risks deriving from the use of information technology, the institutions shall determine its control requirements and rules.*[62] *The institution shall ensure, based on the evaluation of the results of the security risk assessment, in a risk proportionate manner, the following: the controls and processes maintain the resilience, comprehensive and integral protection of the IT security system;*[63] *the operating processes of the production system are regulated, documented and reviewed at a frequency in accordance with the relevant regulations;*[64] *access by end-users to the production system is regulated at both application and infrastructure level, and documented and tested with the frequency determined in the relevant regulations;*[65] *privileged access to the production system is controlled, documented and reviewed at a frequency determined in the relating regulations;*[66] *remote access to the live operational system is controlled, documented and reviewed at a frequency determined in the relevant regulations; remote access to the live operational system is controlled, documented and reviewed at a frequency determined in the relevant regulations;*[67] *the data communication and system connections are documented and reviewed in order to guarantee the confidentiality, integrity and authenticity of data communication;*[68] *the protection of the storage media of the live operational system is controlled, appropriately limited, and the limitations are also maintained by performing regular supervisions and inspections.*[69]

13.1.2. The institution defines the requirement of an independent, regular, comprehensive auditing of IT security within its set of internal information security management system. Independence means that the audit area cannot be involved in the design, selection, implementation or operation of the control measures to be audited and it is not subordinated to the controlled area.

13.1.3. The institution ensures the independent and regular audit of IT security, as defined in the regulations, in such a way that all areas are subject to audit no later than every 3 years.

13.1.4. The financial institution ensures carrying out at least the following audits during the regular audit of IT security:

a) the processes of operations are executed and documented in accordance with the regulations;

b) user access and access rights are adequately regulated and documented, the access set in the systems comply with the authorised access requests and the regulations for conflict of interest;

c) remote access is granted according to the regulations and documentation (of the authorization process);

d) data communication and system connections have been set up in accordance with the documentation, the changes are properly documented and authorised, documents and settings are suitable for ensuring the confidentiality, integrity, and authenticity of data communications, and the auditability thereof;

e) vulnerability scanning of systems is performed as follows: in the case of internal and segregated network zones at least annually in accordance with the process specified in the

[62] Bszt. 12. §, subsection (4), Mpt. 77/A. §, subsection (3), Öpt. 40/C. §, subsection (3), Gov. Decree 2. §, subsection (3)
[63] Bszt. 12. §, subsection (6), paragraph b), Mpt. 77/A. §, subsection (5), paragraph b), Öpt. 40/C. §, subsection (5), paragraph b), Gov. Decree 3. §, subsection (2), paragraph b)
[64] Gov. Decree 5/B. §, paragraph b)
[65] Gov. Decree 5/B. §, paragraph e)
[66] Gov. Decree 5/B. §, paragraph g)
[67] Gov. Decree 5/B. §, paragraph h)
[68] Gov. Decree 5/B. §, paragraph j)
[69] Gov. Decree 5/B. §, paragraph n)

institution's internal rules; in the case of credit card systems, web-based customer service systems, mobile applications, and background systems, scans are conducted at least quarterly; critical errors identified as risks are remediated with no undue delay, non-critical errors are corrected according to a risk-proportionate schedule;

f) penetration testing of applications accessible from the Internet is performed after the correction of errors identified as a risk, prior to go-live, or during any changes impacting security, and then repeated at least annually;

g) for all system components the settings are periodically reviewed and unsecure or unnecessary services, such as scripts, drivers, ports, services, are deleted or disabled;

h) security patches for IT system components and software, depending on the risks, and after the preliminary test in operation, the manufacturer patches are installed, or the institution provides compensating controls.

13.1.5. Exemplary practice

The institution may perform control measures more frequently than required, may carry out other audits in addition to the above to maintain IT security continuously.

13.2. IT monitoring system

13.2.1. Pertinent legal provisions: *the institutions shall set up and continuously operate an IT monitoring system for supervising the safe operation of their information system.*[70]

13.2.2. The institution shall set up its automatic IT monitoring system in a way to be able to ensure that IT system failures are detected and corrected in accordance with the availability times defined in the business continuity plan. To ensure this, the institution:

a) operates a user support organisation;

b) operates an automatic monitoring and alarm system that is capable of the immediate alerting of at least the requirements of paragraphs 6.2.2, 14.2. and IT incidents;

c) defines alerts so that the incidents detected can be managed within the expected recovery time during and outside business hours.

14. LOGGING

14.1. Pertinent legal provisions

The institution shall ensure, at least in a manner commensurate with the security risks based on the evaluation of the results of the security risk assessment, a security environment which logs the events of processes regarded as critical from the aspect of the operation of the information system, furthermore the institution shall ensure that the system is suitable for the regular (and possibly automated) and substantial analysis of logs, and also enables the management of non-regular events.[71] *The system shall monitor all changes of protected information by applying appropriate technical and procedural solutions which shall ensure that even authorised general and privileged users are unable to delete or modify the log or other monitoring information.*[72] *The institution, based on the evaluation*

[70] Bszt. 12. §, subsection (5), Mpt. 77/A. §, subsection (4), Öpt. 40/C. §, subsection (4), Gov. Decree 3. §, subsection (1)
[71] Bszt. 12. §, subsection (6), paragraph d), Mpt. 77/A. §, subsection (5), paragraph d), Öpt. 40/C. §, subsection (5), paragraph d), Gov. Decree 3. §, subsection (2), paragraph d)
[72] Gov. Decree 5/A. §, subsection (3), paragraph c), subparagraph cb)

of the results of the security risk assessment, shall ensure at least the controlled, verifiable and regularly verified user administration of the system (access levels, individual entitlements and their authorisation, responsibilities, access logging, unusual events).[73] *End user activities in production system shall be logged and automated alerts shall be generated for unusual events; events of activities performed through privileged access to production system are logged, the integrity of the log files shall be ensured, and automatic warnings of critical unusual events are generated.*[74]

14.2. General requirements

The institution documents (logs) changes of critical information to be protected, and defines the rules of logging so that monitoring and log interpretation can be done immediately, and alerts are generated in case of unusual changes. The institution ensures the integrity of the log files, ensures the continuous evaluation of logs, and enforces compliance with logging policies by technological solutions as well.

14.3. Regulation of logging

14.3.1. The institution in its information security management system defines the regulation of the monitoring (logging) and reviewing (evaluation) of the critical protected information. As part of this the institution:

a) defines in its information security management system how the operational instructions are prepared, documented and reviewed regarding the following: log settings, parametrisation, logged events (per system type and the minimum sufficient content of log data for critical systems), including data network devices, IT security and other monitoring systems;

b) the IT operations, IT security and business area, in co-operation, define and document the IT security events that need to be detected, and specify the conditions for detection, log retention (storage space, time, method) and the integrity of logs;

c) in its logging policy specifies the method, frequency, time, responsible person, method of reporting of each log file, as well as the events to be monitored, the scope of notifications, the cases and the procedure of immediate alert.

14.3.2. The institution's regulation of logging and monitoring covers at least the logging and log evaluation of:

a) access to operating systems, IT network, servers, application systems, databases, folder structures, IT and network components;

b) changes to customer and financial sector secret data (including transaction data) in its application systems;

c) settings and parameterization of information and network system elements.

14.3.3. The institution also enforces the provisions of the logging regulations with technological solutions, and ensures the integrity of the log files.

14.4. Alerts, immediate response

The institution shall ensure the conditions for immediate response to events requiring immediate alert during the monitoring (logging) and review (evaluation) of critical information to be protected.

---

[73] Bszt. 12. §, subsection (6), paragraph c), Mpt. 77/A. §, subsection (5), paragraph c), Öpt. 40/C. §, subsection (5), paragraph c), Gov. Decree 3. §, subsection (2), paragraph c)

[74] Gov. Decree 5/B. §, paragraphs f) and g)

14.5. Exemplary practices

14.5.1. The institution considers and decides, with a risk-proportionate approach, on the central collection and the automated or central operator managed evaluation of log entries.

14.5.2. In case of implementing a central automatic evaluation system, the institution shall ensure full testing prior to go-live and, and after the successful testing it shall retain the log evaluation unchanged until the full implementation to production.

15. REVIEWING OF OUTSOURCED ACTIVITY

15.1.1. The institution reviews the contractual performance of the outsourced activity in the manner and with the regularity specified by the outsourcing contract and the sectoral laws.[75] During the review the institution takes into account the provisions of the MNB's recommendation on the use of external service providers, if it falls within the recommendation's scope.

15.1.2. The institution and the external service providers shall stipulate in or in connection with their contract pertaining to the outsourced activities the policies that shall be defined by the external service providers at a minimum, which shall be reviewed by the institution during the review of contractual performance.

15.1.3. As part of the contractual performance review the institution assesses the risk analysis of the outsourced activity, documents the results of the assessment, which is evaluated by the management.

15.1.4. As part of the contractual performance review the institution obtains assurance on the adequacy of business continuity procedures of the outsourced activity, whether they ensure the service continuity requirements of the institution.

16. FUNCTIONAL SUITABILITY REQUIREMENT OF THE IT SYSTEM

16.1. Pertinent legal provisions

All the software together shall be suitable for recording the data needed for operation and prescribed by law, the secure registration of funds and financial assets, connecting directly or indirectly to national information systems related to the institution's activity, also including the notification of payment accounts to the company court, use for inspecting stored data, and logical protection commensurate with the level of security risks, and the protection of integrity.[76]

16.2. General requirements

16.2.1. The application systems of the institution comply with the relevant financial and accounting requirements, especially:

a) the financial transactions are recorded in a strictly logged manner, in time sequence (where the chronology can be accurately justified, even can be compared to other transactions) and the subsequent modification of closed transactions is not allowed, but only by following the regulation on cancelling entries, and the documenting thereof (e.g. special permission, logging, record keeping, etc.);

[75] Bszt. 81. §, subsection (1), Hpt. 68. §, subsections (6) and (10), Mpt. 77/B. §, subsections (5) and (9), Öpt. 40/D. §, subsections (5) and (9)
[76] Bszt.12. §, subsection (10), Mpt.77/A.§, subsection (8), Öpt.40/C.§, subsection (8), Gov. Decree 4. §, subsection (2)

b) logs both business and security-related transactions;

c) the internal user and access rights management system enables the separation of financial transactions according to roles, the separation of conflicting roles, including the separation of security administration and business operations;

d) suitable for retrieving the stored data and logs directly from the IT system in case of a review without delay.

16.2.2. The institution prepares its system in due time for the changes of national level IT systems, and the changes of regulations, to satisfy business requirements, an in case of developments it explores the opportunities of technological progress already in the planning phase, and also takes into account the IT security requirements, including the continuity of service.

16.3. Security of the customers' data, property, and financial assets

16.3.1. The institution ensures that the identity and the real intention of the customer are clearly identifiable for every electronic transaction performed by the customer pertaining to the customer's data, financial sector secrets or assets managed by the institution in the system provided by the institution.

16.3.2. The institution continuously monitors the transactions performed by customers, and performs transactions that are considered suspicious based on criteria specified by the risk analysis (e.g. transactions, purchases that are unusually large, or initiated from distant locations within a short time) only after additional customer authentication (e.g. telephone identification, SMS code).

16.3.3. The institution ensures that the customer may provide generally applicable, personalised rules based on their online behaviour and habits at all times.

16.3.4. The financial institution that accepts card payments monitors the activities of online merchants and operates a fraud detection system to detect and prevent abuse by the merchant.

16.3.5. The institution defines default thresholds for electronic transactions and enables the customer to change these thresholds.

16.3.6. The institution offers the customer the opportunity to disable certain electronic services.

16.3.7. Based on prior request of the customer the institution sends the customer instant notification of changes in the balance of accounts selected by the customer, and their personal identification data.

16.3.8. When sending information or validation message (e.g. SMS) to the customer, the institution ensures that the customer can understand what exactly the customer is being informed of and what transaction is actually being performed by the customer. At the same time, the message complies with the principle of data minimization at all times.

16.3.9. In case the institution transmits personal data or financial sector secret via an insecure channel (e.g. e-mail notification) to the customer, the notification is encrypted prior to transmission. The institution also provides the customer with the application and the key required to decrypt the encryption via a different transmission channel prior to transmission.

16.3.10. The institution provides real-time opportunity to the customers to check the status of transactions and account balances at all time.

16.3.11. The institution ensures the non-repudiation of transaction messages on the customer's side with electronic signature and timestamp or confirms the existence of messages with electronic signature and timestamp at the moment of arrival or sending on the server side.

16.3.12. The institution authenticates its electronic transaction messages and ensures their secure storage, and ensures that they can be retrieved and their authenticity can be proven for the period required by pertinent legal regulations.

VI. FINAL PROVISIONS

17. Recommendation is a regulatory tool with no legal binding force for the institutions, issued in accordance with article 13 paragraph (2) point i) of Act CXXXIV of 2013 on the Magyar Nemzeti Bank. The content of the recommendation issued by MNB represents the requirements imposed by law, as well as the principles, methods, market standards and rules proposed for application based on the law enforcement practice of MNB.

18. MNB monitors and evaluates compliance with the recommendation among the supervised financial institutions falling within the scope of authority of MNB, in line with general European supervisory practices.

19. MNB brings to the attention of the financial institutions that it can incorporate the recommendation into its policies. In this case the financial institution has the right to indicate that the respective policy is in compliance with the pertinent recommendation issued by MNB. If the financial institution wishes to incorporate only certain parts of this recommendation into its policies, then it shall avoid referring to the recommendation, or it shall apply this referral only to the parts actually incorporated.

20. MNB expects the application of this recommendation by the concerned financial institution beginning on 01/01/2021, and the MNB considers it a good practice that the financial institutions take into account the expectations contained in the present recommendation in their new developments or developments ongoing at the time of the publication of the recommendation.

21. Recommendation 7/2017 (VII. 5.) of the Magyar Nemzeti Bank on the protection of information systems, and recommendation 15/2015 of the Magyar Nemzeti Bank on the safety of financial services provided online are repealed on 01/01/2021.

Dr. György Matolcsy

President of the Magyar Nemzeti Bank

In case of discrepancies between the language versions, the Hungarian version shall prevail.

Appendix 1. of the Recommendation 8/2020 (VI. 22.) of the Magyar Nemzeti Bank

Table of contents

Appendix 2. of the Recommendation 8/2020 (VI. 22.) of the Magyar Nemzeti Bank

References to the Government Decree