Recommendation 4/2019 (IV. 1.) of the Magyar Nemzeti Bank
on the usage of community and public cloud computing services

TRANSLATION

I. Objective and scope

The objective of this recommendation is to provide practical guidance to entities in the financial intermediary system for managing the risks arising from the use of community and public cloud computing services and for the uniform interpretation of relevant national and European Union (henceforth: EU) legislation and other regulatory instruments.[1]

To this end, the recommendation – based on the lifecycle of cloud computing services and on relevant security principles – defines the minimum contractual requirements, describes the risks to be managed and the expected control measures, and provides information on the main aspects of supervisory reviews pertaining to the scope of present recommendation conducted by the Magyar Nemzeti Bank (henceforth: MNB) acting in its role as supervisory authority of the financial intermediary system.

MNB – based on the good practices and requirements set out in the recommendations of the European Banking Authority (henceforth: EBA) on outsourcing to cloud service providers (EBA/REC/2017/03) – defines its requirements in connection with the use of community and public cloud computing services for all entities of the financial institutions intermediary system.

This recommendation is addressed to the entities and persons (henceforth together: entity) defined in Section 39 of Act CXXXIX of 2013 on the Magyar Nemzeti Bank wishing to use cloud services.

This recommendation does not comprehensively refer to the legislation when defining principles and requirements, but the addressees of this recommendation still need to comply with the respective legal provisions. This recommendation should be implemented in addition to sectoral and other relevant laws and recommendations. The recommendation should be applied together with the MNB recommendation 7/2017 (VII. 5.) on information system protection and the MNB recommendation 15/2005 on the security of online financial services.

II. Definition of cloud computing

1. Cloud computing is a solution that enables network access to shared, configurable computing resources (e.g. networks, servers, storage devices, applications and services) on demand, which can be provisioned quickly, with minimal management effort or interaction from the cloud service provider (henceforth: CSP).[2] The solution has the following five main characteristics:

    a) The service can be used on demand, even on a self-serve basis;

    b) General network access (through the Internet or a private network);

    c) Shared resource usage. The service provider serves several customers (in a multi-tenant model) and allocates the various physical and virtual resources dynamically on-demand. Customers generally

[1] See the Appendix for the list.

[2] The definition of cloud services used in this guideline is based on the following document of the American National Institute of Standards and Technology (henceforth: NIST): *The NIST Definition of Cloud Computing (SP 800-145)*
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

do not know and cannot influence the exact location of the resources in use, however, they may define it at a higher abstraction level (e.g. on a country, region or data centre level);

d) Fast reaction to changing capacity needs;

e) Measured services (usage-proportionate fees).

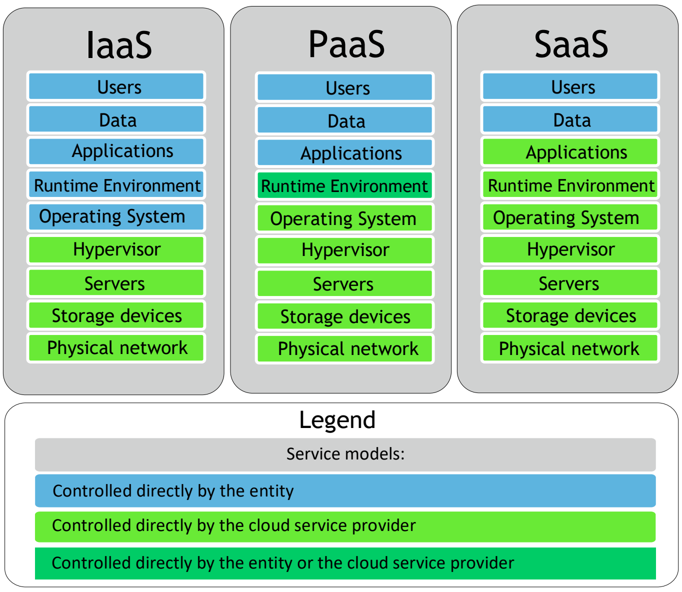
2. This recommendation is relevant to the public and community cloud models, as well as to the public or community elements of the hybrid clouds, out of the four main cloud access models. Public cloud means a cloud service available to any customer, whereas community cloud means a cloud service jointly available to several, even independent entities based on an organising principle (e.g. members of a supply chain, groups of companies or government entities). Hybrid cloud utilises at least two distinct cloud infrastructures with different deployment models, between which data and services can move on demand.
3. The cloud can be accessed by one of three service models:

a) Infrastructure as a Service (IaaS): the service provider provides virtual hardware, and the customer installs and operates all software on it.

b) Platform as a Service (PaaS): the service provider provides virtual hardware and platform software (usually operating system, database software, web server and application server), and the customer installs and operates its own business applications.

c) Software as a Service (SaaS): the service provider provides a business solution operating on a virtual hardware and platform software; which is configured and partly operated by the user (e.g. user access management).

4. The following chart shows who is in control of the individual service elements in each service model:



IaaS	PaaS	SaaS
🟦 Users	🟦 Users	🟦 Users
🟦 Data	🟦 Data	🟦 Data
🟦 Applications	🟦 Applications	🟩 Applications
🟦 Runtime Environment	▨ Runtime Environment	🟩 Runtime Environment
🟦 Operating System	🟩 Operating System	🟩 Operating System
🟩 Hypervisor	🟩 Hypervisor	🟩 Hypervisor
🟩 Servers	🟩 Servers	🟩 Servers
🟩 Storage devices	🟩 Storage devices	🟩 Storage devices
🟩 Physical network	🟩 Physical network	🟩 Physical network

Legend

Service models:

🟦 Controlled directly by the entity

🟩 Controlled directly by the cloud service provider

▨ Controlled directly by the entity or the cloud service provider

Picture 1.: Service models and the parties in control of service elements

III. Lifecycle of cloud service usage

5. It is the entity's responsibility to identify the risks and compliance requirements in all phases of the cloud service's lifecycle, and to implement proportionate protection measures by considering at least the following aspects.

III.1. Identifying the business needs, decision support and planning

6. Using cloud services may be considered for addressing certain business requirements and owners' expectations pertaining to information technology (such as cost reduction, flexibility, volatile capacity requirements, CAPEX reduction, or quick implementation). In this case the entity examines the viability of using cloud services, taking into consideration business needs, costs and risks, security requirements and legal requirements. MNB recommends that preparation for decision and planning shall be done as follows.

III.1.1. Ensuring legal compliance of cloud services

7. Prior to using cloud services, the entity ensures that full regulatory compliance can be achieved for using those services. The responsibility for operating in compliance with regulations remains with the entity while using cloud services, therefore the entity assesses beforehand how it can meet its obligations, and how the CSP ensures the necessary controls for the entity and provides monitoring capabilities.
8. When applying this recommendation special attention needs to be paid to data that can identify customers directly or indirectly, or data that can be used for profiling customers (henceforth: customer data), and data containing tax, trade, banking, securities, fund, payment, insurance or occupational pension secrets (henceforth: financial sector secret). The entity defines suitable guarantees for handling, processing, and storing data while using the cloud service in line with respective national laws and EU legislation. These guarantees, among others, ensure among others that all data that qualify as customer or financial sector secret will be handled, processed and stored by the handler or processor only to the extent and time necessary to achieve the purpose of handling the data, according to the principle of purpose limitation.
9. If the cloud service involves the handling, processing and storing of personal data, the entity ensures compliance with international and national regulatory requirements on data handling and processing.[3]
10. The entity assesses whether using the cloud services qualifies as outsourcing according to applicable financial sector laws.[4] Based on the assessment the entity makes a documented decision whether it treats the service as outsourcing, in line with relevant legal provisions. In case a provision of the present recommendation uses the term "outsourcing", the provision relates to those cases of cloud services that qualify as outsourcing according to the applicable sectoral laws.
11. If the entity or the system used by it has been identified as essential in the European or national financial sector, then the entity takes into account the relevant legal provisions.[5]

[3] See section 2. of the Appendix for the list of regulations.

[4] See section 1. of the Appendix for the list of regulations.

[5] See section 4. of the Appendix for the list of regulations.

III.1.2. Pro-con analysis

12. In order to make a well-founded decision on using cloud services the entity performs a pro-con analysis that covers at least the following:

    a) Analysis of other (non-cloud-based) solutions that satisfy the business need, which encompasses the assessment of the risks associated with the service by considering the potential losses and the estimated cost of controls (e.g. costs of service level agreements, audits, accreditations, or additional security services);

    b) The cost and the risks of introducing the cloud services (e.g. application and data migration);

    c) The options for and the estimated cost of abandoning the cloud and downloading the data from the cloud.

III.1.3. Assessment of material activities

13. MNB recommends considering the following as good practices in assessing material activities: the definition of material activities is defined by guideline 1(f) of the Guidelines on outsourcing of the Committee of European Banking Supervisors of 14 December 2006, whereas the requirement of assessing material activities is defined by guideline 4. Detailed evaluation criteria are defined by section 4 paragraph 1 of EBA's Recommendations on outsourcing to cloud service providers (EBA/REC/2017/03).

14. The entity regards at least the following activities material in connection with cloud services:

    a) Activities of such importance, whose deficiency or outage prevents or endangers regular operation, contingency of business or providing services;

    b) Activities that require a licence from a supervisory authority;

    c) Activities that significantly impact risk management;

    d) Management of risks related to the above activities.

15. The entity assesses the materiality of activities impacted by the cloud services based on the following criteria:

    a) The criticality and the risk of the activities regarding the entity's viability, its ability to continue its business, and the entity's obligations to customers;

    b) The operational, legal, reputational and financial risks of the activity's outages;

    c) The impact of incidents on the confidentiality, integrity and availability of data involved in the activities.

III.1.4. Register of activities involved in cloud services

16. The entity maintains an up-to-date register of all activities involved in cloud services used by the entity and its group – regardless of their materiality – that impact the data of the entity, with special attention to customer data. Regarding the register of information MNB recommends considering section 4 paragraph 5 of EBA's Recommendations on outsourcing to cloud service providers (EBA/REC/2017/03) as a good practice, which recommends additional data to be captured on top of the data that needs to be reported to MNB based on paragraphs 29. a)-g) of present recommendation.

III.2. Cloud services risk analysis

17. MNB recommends that the entity's IT risk analysis – which includes risk assessment (identification and evaluation of risks in line with the service model applied), as well as designing risk mitigating measures – should cover the options for implementing the provisions listed in this paragraph and paragraphs 37-59. for all phases of the service's lifecycle. MNB regards it as good practice that the entity either operates its own controls in a risk proportionate manner or stipulates in the contract that the service provider should operate the controls – and the entity obtains assurance on the operation thereof – so that these requirements are met, in line with the applied service model and the materiality (confidentiality, integrity, availability) of impacted services. MNB recommends that the entity performs its risk assessment as described below.
18. The management of the entity ensures that risk reduction action plans[6] are prepared, the prerequisites for the implementation are in place, and that the measures taken are monitored. The entity shall manage risks causing regulatory noncompliance with risk mitigating measures (controls); that is, such risks cannot be transferred or accepted.

III.2.1. Location of data and data handling[7]

19. The entity assesses the legal, political, economic, security and supervisory risks in connection with the data and data categories and the location of handling, processing and storing data involved in the cloud service. The entity accepts only a level of risk that does not cause regulatory noncompliance and is in line with the materiality of the activity, and the confidentiality, integrity and availability requirements and expectations of data involved in the cloud service. The entity takes special care while using cloud services outside the European Economic Area due to data protection risks and geopolitical risks endangering effective supervisory activities.[8] In such cases the entity proves in a documented manner that it has considered the applicable provisions for handling data in a third country.

III.2.2. Exit risks

20. The entity assesses and manages the risks of abandoning (exiting) a cloud service, including the possibility of an unexpected, unplanned exit, for example if the service provider is terminated or the service is discontinued. The entity prepares a cloud service exit strategy and an action plan to mitigate the risks.
21. As part of the exit strategy:
    a) The entity stipulates service conditions that allow the exit from the cloud without difficulty (see paragraph 35.), especially regarding the provision of stored data in a format that can be interpreted and used independently of the cloud service (portability);
    b) Ensures and tests the operability of the impacted business processes in case the cloud service is discontinued with a risk proportionate method and frequency.

[6] The requirements in connection with the action plans are contained in the MNB recommendation no. 7/2017. (VII. 5.).

[7] Respective legislative requirements are defined in detail in the regulations listed in section 2. of the Appendix.

[8] In case of cross border cloud services, the managing of the risks related to the service provider's geographical location – including data protection risks – is described in Guideline 4. (paragraph 4) of the Guidelines on outsourcing of the Committee of European Banking Supervisors of 14 December 2006; respective criteria are contained in section 4.6 of EBA's Recommendations on outsourcing to cloud service providers (EBA/REC/2017/03).

III.2.3. Assurance

22. The entity documents the level of assurance it deems necessary on the effectiveness of the CSP's risk mitigation measures in its control environment for the services provided.
23. Methods of obtaining assurance and their corresponding assurance levels are as follows:

    a) Contractual obligations, declarations or professional indemnity insurance of the CSP (medium level of assurance).

    b) CSP commissioned independent third-party audit reports or certifications of a relevant international standard[9] (medium or high level of assurance depending on the reputation[10] and expertise of the third party and the acceptance of the certificates).

    c) Audits conducted directly by the entity or indirectly, based on audits commissioned by the entity, or certifications of the CSP performed by independent third parties (medium or high level of assurance depending on the cloud security expertise and experience of the auditors)

24. The entity strives to achieve the possible highest level of assurance in line with the criticality of the activity and documents this level. If the entity wishes to obtain assurance through its own audits, then it provides for cloud security and audit resources with adequate expertise.

III.3. Contractual requirements

25. MNB expects that the entity, while complying with relevant legislation, ensures that the following are contractually defined and stipulated, in line view with chapter IV:

    a) A clear procedure for the modification of service conditions or other contractual terms; contract extension; and the introduction of new functions, additions, related software and services.

    b) Detailed conditions of contract termination initiated either by the entity or the service provider; and detailed regulation of the right to terminate (ordinary notice, extraordinary notice), including the destruction of data.

    c) The termination notice period and the procedures for returning and deleting data, defined based on the information risk assessment and the business needs, so that the discontinuation of the service can be carried out safely and business processes do not suffer an unacceptable level of disruption.

    d) The right to audit by the entity, its agents, and the MNB as well, regarding the service provider and the provided service, including the right to perform on-site inspections.

    e) If relevant to the entity, the right to certify the services provided by the CSP based on 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.

    f) Provisions for contractual guarantees provided by the CSP, warranties, and compensation for damage, with special attention to that the guarantees shall be commensurate with the potential damages.

[9] For example: ISO 27001, ISO 27017, ISO 27018, ISAE 3000, ISAE 3400, ISAE 3402

[10] Assessment criteria of independent parties for example, but not limited to experience and references obtained in similar investigations; positive client feedbacks; liability insurance with sufficient scope, extent and value; relevant certifications; financial stability; code of ethics; presentations on professional events; relevant experience, education and qualifications of employees delegated to the certification engagement.

g) Events deemed Force Majeure and the procedures to manage them.

h) Handling of commercial licenses and intellectual property.

i) Language, form, conditions and content of the service and the respective communication.

j) Information security and data protection roles and responsibilities, with special attention to obligation to inform and potential service chains.

k) Defining the exact locations – at least on a data centre level – of data handling, processing and storing.

l) Defining suitable guarantees for handling, processing, and storing data in line with respective national laws and EU legal instruments to ensure that all data that qualify as customer or financial sector secret will be handled, processed and stored by the handler or processor only to the extent and time necessary to achieve the purpose of handling the data.

m) Defining the requirements for the protection and safe operation of resources.

n) Setting out service level agreements (SLA-s) by taking into account at least the following:

   na) Indicators to be measured, and their expected values;

   nb) Methods and tools for measurement;

   nc) Service availability and minimal functionality;

   nd) The entity performing the measurements; the responsibility for writing SLA reports; frequency of the reports;

   ne) Consequences of violating the SLAs in line with the damages; and escalation procedures.

o) Expectations regarding the processes operated by the service provider, including security management, operation and development, as well as the security expectations regarding human resources;

p) Security incident management procedures, including the service provider's obligation to report security incidents impacting the service and the service provider in connection with the cloud service provided without delay;

q) The requirement for the service provider to provide support and data for investigating frauds perpetrated at the entity.

III.3.1. Service chain

26. MNB considers it justified for the entity to assess the risks in connection with the service chain, which are related to the service provider involving others (further service providers, subcontractors, vendors, henceforth: subcontractors) in providing the service. MNB expects the entity to involve services provided through chain outsourcing only if the subcontractor fully satisfies the contractual obligations between the entity and the outsourcing service provider, with special attention to the provisions ensuring the right to audit of the supervisory authority (including the right for onsite inspection). [11]

27. MNB expects the entity to stipulate the following in the contract with the service provider:

[11] Requirements for the service chain and chain outsourcing are defined by guideline 10. of the Guidelines on outsourcing of the Committee of European Banking Supervisors of 14 December 2006. Detailed requirements are defined by section 4.7. of EBA's Recommendations on outsourcing to cloud service providers (EBA/REC/2017/03).

a) The roles, responsibilities and accountability of all subcontractors that can access or are involved in the process of handling and processing data shall be readily identifiable and transparent to the entity.

b) The service provider shall inform the entity prior to significant changes to subcontractors involved in providing the service, in a manner that allows the entity to perform a risk assessment before the change enters into force.

c) The entity may terminate the service contract if the change to the subcontractors has an adverse effect to the risks of activities involved in using the cloud service.

d) The usage of subcontractors by the service provider shall not impact the contractual obligations, roles and responsibilities of the service provider.

28. MNB expects the entity to review and monitor the used cloud services in the entire service chain.

III.4. Reporting to the MNB

29. MNB expects the entity – in addition to the requirements of applicable laws, and together with them – to provide information on all activities involved in the use of cloud services according to the following criteria:

a) the details of the cloud service provider’s parent company, if applicable (including name, address, tax number);

b) a description of the activities, data and data categories to be outsourced;

c) the country or countries where the service is to be provided (including the location of handling, processing and storing of data);

d) the commencement date of the contract in effect;

e) the next contract renewal date (where applicable);

f) the applicable law governing the contract;

g) the contract and its appendices;

h) the materials of the decision making, especially the following: pro-con analysis, materiality assessment, risk assessment, the assessment where the entity had determined whether the service qualifies as outsourcing, documents of the decision, exit strategy.

III.5. Implementation of a cloud service

30. MNB considers it justified for the entity – in view of chapter IV. – to ensure that at least the following tasks are performed if applicable to the respective cloud service implementation project.

III.5.1. Preparation for the implementation

31. The entity performs the following steps during the preparation for the implementation, and documents them in a simple and appropriate manner:

a) Defines its business, functional (e.g. versions and modules), technical (e.g. IT and security) and control environment requirements, and the compliance with them.

b) Defines the development, testing, migration and transition requirements pertaining to the implementation of the service, as well as the go-live and service acceptance criteria, and documents these in an auditable manner.

c) Creates a migration strategy, including scheduling, IT and security requirements, tools to be used, as well as a detailed implementation plan.

d) Defines the co-operation requirements, tasks and responsibilities of the service provider in performing the migration.

e) Defines detailed service specifications, test cases and test scenarios, and defines and tests a plan for managing extraordinary events during migration (back-out plan).

f) Defines the acceptance criteria for the go-live, and the related responsibilities.

III.5.2. Performing the implementation

32. The entity performs the following steps during the implementation, and documents these in an auditable manner:

a) Implements the tools for the migration.

b) Prepares a schedule containing elementary steps, by defining milestones and resources, appointing those responsible, during which also prepares for a worst-case scenario.

c) Runs functional, module, regression and security tests in a test environment using test data; documents the results of the tests, with special attention to correcting critical errors.

d) Based on the test results decides to go-live or to postpone the go-live until errors are rectified.

e) Performs the migration in the production environment following the steps of the migration plan.

f) Performs validation and checks the correctness of the migrated data based on the acceptance criteria. If according to the entity’s risk analysis the migration involves critical functions or systems, then the entity engages an independent and competent party to validate the migration based on completeness, integrity and confidentiality criteria.

III.6. Continuous monitoring of the service

33. MNB considers it justified that for the sake of proper monitoring and auditing the service the entity itself applies the requirements defined in chapter IV. or ensures that the CSP complies with them while employs cloud services for its operations, with special attention to the following:

a) Setting up an effective and coordinated incident management process between the entity and the service provider;

b) Regular testing of disaster recovery (DR) plans;

c) Monitoring the service provider’s financial viability, and compliance with SLAs;

d) Logging the events based on the results of a risk analysis, ensuring the integrity of logs and analysing the logs;

e) Updating the cloud services risk analysis at least with the frequency prescribed by law, or at an equal or higher frequency stipulated by the entity’s policies, concurrently with the information security risk assessment, or in case of a significant change of the data categories and functions involved in the cloud service.

f) Using only officially released, tested and supported service versions;

g) Using only data centre locations that comply with domestic and EU requirements and have been formally accepted.

h) Preparing for faulty performance; assessing alternative cloud service providers or other solutions to ensure business continuity.

i) Regularly updating the exit strategy and action plan.

III.7. Exit

34. MNB deems necessary that the entity in the cloud service exit phase carries out the exit strategy and action plan defined in paragraph 20, in line with the process described below.

III.7.1. Preparations for the exit

35. In the preparation phase of the exit the entity makes available the required personnel, assets and technology for the exit, as well as the required legal and contractual conditions, including the following:

a) The infrastructure required for returning the data and take-over of service so that the business processes relying on the affected systems can operate without interruption, or with a level of disruption that can still be tolerated by the business needs.

b) The expertise and project team necessary for exiting from the cloud service and resuming local operations or transferring the service to another provider.

c) The detailed exit implementation plan, including the scheduling of the exit, the IT and security requirements, the tools to be used, the test cases and scripts, as well as the acceptance criteria for the testing and for the service taken back or migrated to another service provider.

d) A detailed step-by-step time schedule by defining milestones and resources, assigning responsibilities, including a worst-case scenario.

e) The co-operation obligations, tasks and responsibilities of the entity and the CSP in discontinuing the service.

f) The scheduling and the conditions of providing the service and the availability and transfer of data during the exit.

III.7.2. Performing the exit

36. The entity performs the following steps defined in the exit strategy and action plan in a documented manner:

a) Installation of migration tools.

b) Transferring data to the target system taking into account the provisions defined in section IV.1.1.

c) Testing the data migration into a test environment.

d) Live data reload into the production environment and performing the takeover of the service following the scripts.

e) Validation based on the acceptance criteria; verifying the correctness of the data taken back; and closing the migration.

f) Follow-up for fixing errors after migration.

g) After the successful exit from the cloud, deleting the data managed by the former service provider, including both live, backup and archive environments per contractual conditions. The service provider shall provide assurance (declaration) on the execution of the data deletion.

h) Terminating the unnecessary IT and communication connections with the service provider.

i) Reporting the exit to the MNB.

IV. Cloud service security principles

37. MNB recommends that the entity take the following cloud service security principles and implementation steps into consideration and obtain assurance that the service provider complies with the provisions within its scope of authority, pursuant to paragraphs 17-25.

IV.1. Data security, data and secrecy protection

38. MNB recommends that as a prerequisite to data security, data and secrecy protection, the entity carry out the following:

    a) Identifies and applies security classification to the data involved in the cloud service in line with applicable law and its own data protection policy;

    b) Defines data security and protection requirements per the security classification of the data, pursuant to relevant regulations.

39. When defining technical data security and protection requirements and during the use of the service, the entity uses risk-proportionate and state-of-the-art technical solutions (e.g. algorithms, protocols and parameters), which are internationally accepted as safe.
40. The entity obtains assurance regularly of the CSP's full compliance with data security and protection requirements – at least annually, or after significant changes in the relevant business process, service, configuration or legal environment. The entity may rely on independent third parties' audits or certifications for obtaining assurance according to the provisions defined in section III.2.3., in a risk-proportionate manner.
41. MNB draws attention to the fact that the entity is accountable for the integrity, confidentiality and availability of the data in transit and while being stored.
42. From a data protection perspective, the entity ensures the safe handling and processing of personal and customer data, as well as data classified as secret by financial sector regulations, also in compliance with the data protection regulation in force.[12]

IV.1.1. Security of data in transit

43. The entity and the CSP, in order to maintain the security of data in transit, ensure that data transmissions between the entity and the cloud, between the resources in the cloud, and between the cloud and other external service providers are protected from unauthorised access and modification; along with the availability and the required bandwidth of the network connections.

[12] See relevant regulations listed in the Appendix.

44. The entity and the service provider ensure the following for the system components that fall within their scope of authority based on the service model:

    a) Provide encryption and integrity protection of data transmissions. The entity takes further risk-proportionate measures in addition to the line encryption and integrity protection provided by the telecommunications service providers;

    b) Ensure the authentication of the assets and users involved in communication;

    c) Ensure the availability and fault tolerance of network connections and the network bandwidth required for normal operation in line with the expected service levels.

45. The requirements defined in paragraphs 43-44. also apply to data transmission generated by service and system management processes.

46. In case the data is downloaded from or uploaded to the cloud not only through the network, then the confidentiality and integrity control measures defined in paragraphs 43-44. are applicable to the utilised physical data media as well.

IV.1.2. Safety of the data stored

47. The entity and the CSP, in connection with the data stored, in order to protect the dependent business processes, ensure the availability of the data stored in the cloud, and its protection from unauthorised access and modification thereof.

48. The entity and the service provider ensure the following for the system components that fall within their scope of authority based on the service model applied:

    a) They consistently enforce the data security requirements within their scope of authority, for example by establishing adequate logical data access controls (the options vary by cloud service model);

    b) They define the availability parameters of data in line with the expected recovery time objectives (RTO) and recovery point objectives (RPO[13]) of the impacted business processes;

    c) They define the requirements for the safe deletion of stored data, including the tools and processes for deleting backups and archives, and the assurance that the service provider has to provide thereof;

    d) When the entity obtains assurance on compliance with data security requirements within the service provider’s scope of authority, the aspects of assurance should include confidentiality, integrity and availability, along with the safe destruction of data storage devices during disposal;

    e) The entity ensures the independent storage of data backups for functionalities or systems deemed critical by the risk assessment. The frequency of the backups to be stored independently is defined in line with the risks and the regulatory requirements.

IV.1.3. Data protection

49. The entity in order to protect data obtains assurance that the cloud service provider adheres to the relevant data protection rules and legal regulations.

[13] The tolerable period of data loss.

50. For the sake of protecting data the entity ensures the following:

    a) The entity identifies deviations between the pertinent regulatory requirements for data protection and the cloud service provider's data protection commitments, practices and data reporting obligations. When identifying these deviations, the entity:

       aa) Compares the service provider's data handling and data processing practices to the requirements relevant to the entity;
       ab) Assesses when and on what condition the service provider is obliged to provide data to authorities (e.g. based on regulations in effect in the service provider's country), and what notification the service provider undertakes to provide to the entity when it complies with such obligations;
       ac) Assesses whether the service provider's subcontractors and other business partners access the data in accordance with the purpose of handling the data, and when and on what condition can data subjects access the data stored of them. If the entity identifies it as a risk, it does not consent to the involvement of the respective subcontractor or other third party at its discretion. The entity's assessment of the subcontractors does not constitute a right that extends beyond the original purpose of the right to audit.

    b) The entity applies contractual conditions that manage the differences identified, thereby ensuring full compliance.

51. In addition to the laws, European Union legal acts and MNB recommendations listed in the Appendix that govern the data protection measures to be taken by the entity within its own scope of authority, also the recommendations of The Hungarian National Authority for Data Protection and Freedom of Information (NAIH)[14] apply.

IV.2. Protection of resources

52. MNB expects that the entity, in order to protect its resources, obtains assurance that the resources (processing and storage capacities) allocated to it in the cloud are protected against unauthorised physical or logical access, damage and theft. MNB recommends that the entity performs this as described below.

53. For the sake of protecting resources the entity ensures the following:

    a) The entity obtains a high level of assurance on the protection of the CSP's data centres, computing and communication devices, and on the measures ensuring availability.

    b) The entity obtains a high level of assurance on the separation of the CSP's clients and systems.

    c) The assurance covers at least the following, depending on the cloud service model:

       ca) Physical access and environmental controls of physical resources;
       cb) Logical access controls and security settings of the virtualisation infrastructure, including the hypervisor, virtual data storage, virtual networks, as well as the protection of their management tools;
       cc) Logical access controls and security settings of operating systems, middleware, databases and applications, including the use of configurations which have been hardened based on manufacturers' and industry recommendations;

[14] The recommendations of NAIH are available on: https://www.naih.hu/ajanlasok.html

cd) The technical separation of resources belonging to different clients, with special attention to management interfaces (e.g. web-based administrative interfaces, application programming interfaces – APIs);

ce) Management of cryptographic keys, including the use of HSM (Hardware Security Module).

IV.3. Security of IT processes

54. MNB expects that the entity, in order to protect IT processes, implement data security and data protection of cloud services, as well as protection of resources – ultimately the safety of the cloud service – through a regulated, secure and monitored IT governance system and processes, by taking the following into consideration.

IV.3.1. Security management

55. In order to protect IT processes, the entity performs the following security management activities:

a) As described in section III.2.3., the entity obtains assurance on the service provider's information security governance system, processes and the operation of respective controls, or in case of shared responsibility, the entity implements these for the components that fall within its scope of authority, covering at least the following aspects:

aa) Certifying the information security management system (ISMS) based on relevant international standards, if the expected level of obtaining assurance justifies this;

ab) Defined structure of the information security organisation and segregation of duties;

ac) Information security risk management system, including the management of risks associated with human resources. The entity requires the service provider to perform HR risk screening that covers its employees and subcontractors as well, and regular security awareness training;

ad) The operation and the results of internal and external audit functions. The entity requires general security audits, vulnerability tests, penetration tests, and certifications (based on international security standards) to be performed in a risk-proportionate manner;

ae) A quick and effective process for fixing identified security vulnerabilities, and the reporting thereof;

af) Keeping configuration management systems up-to-date;

ag) Managing business continuity, ensuring availability, backup systems, and solutions supporting disaster recovery. The entity requires regular BCP/DRP testing, and the regular updating of the test plans;

ah) Secure architecture planning and network security controls based on best practices;

ai) User and access rights management. The entity requires that only the service provider's authorised staff and subcontractors have access to the resources in the cloud that have been allocated to the entity, based on a documented approval process;

aj) Security logs and monitoring. The entity requires that alerts and log entries are generated about security events and incidents related to the service or the service provider in connection with the service provided, and these are adequately protected and shared with the entity when requested;

ak) Management and reporting of security incidents. The entity should be informed immediately of security incidents and their resolution;

al) Fraud investigation. The entity requires the service provider to support such an investigation, and a regulated fraud investigation process;

am) Protection against malicious codes, including the installation, regular update and central monitoring of security tools, as well as regular antivirus checking of the network and devices;

an) Management of mobile devices, including mobile management tools and end user mobile devices, the identification and registering thereof, as well as the definition and enforcement of respective security requirements (e.g. access protection, encryption, data leakage protection);

ao) The protection of the network parameter, including the definition of a properly regulated network connectivity rule set and its enforcement with technological devices, providing protection against data leakage, as well as intrusion detection and prevention.

b) If available, the entity uses the compliance and security programs operated by the service provider that allow for the following (examples):

ba) A direct connection and communication with the service provider's security and compliance officers and experts, as well as its internal and external auditors;

bb) Reviewing the details of the certificates, risk management and audit reports required for legal compliance;

bc) Submitting the entity's individual requirements for the expansion, improvement, and certification of the control environment;

bd) Using further services that serve safe and transparent operations (e.g. regular penetration testing, joint DRP testing, participation in security forums).

c) If available, the entity uses the extended notification system operated by the service provider for security incidents, which also covers – besides the incidents directly affecting the entity – the events affecting the service provider or other customers of the service provider; furthermore, provide notification of failed (DRP and security) tests as all of these may represent a direct or indirect threat to the entity.

IV.3.2. Operations security

56. In order to protect operations, the entity obtains assurance on the controlled operating of the service provider's IT operational processes, or in case of shared responsibility the entity implements these for the components that fall within its scope of authority, covering at least the following aspects:

a) Definition and documentation of operational procedures and responsibilities;

b) Backup and restoring procedures;

c) Monitoring of operations and log management;

d) Asset management (identification, registration and handling of assets during their entire lifecycle);

e) Change and version management, configuration management;

f) Incident, problem and request management, and the related notification procedures;

g) Management, monitoring and reporting of SLA expectations.

IV.3.3. Security of development

57. In order to ensure the security of development, the entity obtains assurance on the controlled operation of the development processes on the service provided, or in case of shared responsibility the entity implements these for the components that fall within its scope of authority, covering at least the following aspects:

a) Application of documented development guidelines and methodologies, with special attention to secure development methods and practices;

b) Inclusion and documentation of security expectations in developments;

c) Setting up and separating development and test environments;

d) Security and penetration testing prior to going live, and at least annually during live operation;

e) Quality assurance and control of developments performed by subcontractors.

IV.4. User and access rights management[15]

58. MNB – in order to enable the security of user and access rights management – requires the entity to ensure that access to the cloud service is restricted to the necessary and sufficient level in line with the relevant business requirements, by using appropriate identification, authentication and authorisation solutions, by taking into consideration the below.

59. In order to create and maintain a secure user and access rights management the entity and the service provider ensure the following for the system components that fall within their scope of authority based on the service model applied:

a) The entity establishes a documented and approved user and access rights management procedure to control access to the cloud service, which is at least on the same level with the procedure for local systems and encompasses the processes for requesting, approval, and setup of access rights, as well as their regular review and revocation;

b) They consider using multi-factor authentication in a risk proportionate manner, at least for privileged users;

c) The activities of privileged users related to the service are logged, the logs are regularly reviewed; and the entity is also entitled to review;

d) The entity defines conflicting roles and access rights in connection with the cloud service;

e) The entity has comprehensive and up-to-date records of authorised users and their access rights, including privileged, technical and external / remote users, which can be compared with the actual system settings;

f) User and access rights management activities are regularly monitored (who requested, authorised, set, reviewed or revoked what right for whom).

V. Supervisory audit

60. MNB, based on pertinent legal provisions, may audit the control environment of the cloud service at the entity, at the service provider via the entity, as well as at the CSP's subcontractor. The entity is obliged to ensure via contractual conditions that the use of the cloud service does not hinder MNB in performing its duties, and the service provider and its subcontractors co-operate with MNB, and MNB may carry out on-site or off-site investigations at the service provider (the provider of the outsourced activities) and its subcontractor during the audit of the cloud service.

61. The primary purpose of the audit on the cloud service is to determine the following:

[15] This section defines the requirements for the management of users and access rights controlled by the institution. Please see paragraph 55. ai) for the requirements concerning the users and access rights controlled by the cloud service provider.

a) Whether the IT solution required for the smooth operation of the entity and for achieving its business objectives has been provided; as well as whether the conditions required for the ongoing operation and development of this solution have been provided;

b) Whether management has duly identified and evaluated the security risks of the cloud service and its development, implemented risk-proportionate controls, and provided the contractual, regulatory, governance, HR, technical and monitoring conditions required for the continuous operation of those controls;

c) Whether the controls stipulated in the contract operate effectively; what tools are used to ensure their operation and how they are monitored;

d) Whether the entity, the service provider (the provider of the outsourced activities) and its subcontractors comply with legal requirements during the use of the cloud services.

62. To achieve the goals defined in paragraph 61., and with regard to present recommendation, MNB's supervisory audits pay attention to the review of the following:

a) Documents of the decision-making process, especially the pro-con analysis and requirement lists, materiality assessment;

b) Risk analysis and risk mitigating actions;

c) Exit strategy and action plan;

d) Cloud service contracts and their amendments;

e) Definition and enforcement of information security and data security requirements, adequacy of IT controls;

f) Adequacy of the assurance obtained by the entity;

g) BCP/DRP plans and test documents;

h) Independently stored backups.

VI. Final provisions

63. Recommendation is a regulatory tool with no legal binding force for the entities, issued in accordance with section 13. § (2) 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.
64. MNB monitors and evaluates compliance with the recommendation among the entities falling within the scope of authority of MNB, in line with general European supervisory practices.
65. MNB brings to the attention of the entity that it can incorporate the recommendation into its policies. In this case the entity has the right to indicate that the respective policy is in compliance with the pertinent recommendation issued by MNB. If the entity 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.
66. MNB expects the application of this recommendation by the impacted entities beginning on 01/05/2019.
67. By putting this recommendation into effect, the Recommendation 2/2017 (I. 12.) of the Magyar Nemzeti Bank on the usage of community and public cloud computing services is repealed on 01/05/2019.

Dr. György Matolcsy
President of the Magyar Nemzeti Bank

Appendix 1. of the Recommendation 4/2019 (IV.1.) of the Magyar Nemzeti Bank

Certain pertinent laws, recommendations and guidelines

1. Financial sector regulations and European Union legal acts

1.1. Act XCVI of 1993 on voluntary mutual insurance funds;

1.2. Act LXXXII of 1997 on private pension and private pension funds;

1.3. Act CXVII of 2007 on Occupational Retirement Pension and Institutions for Occupational Retirement Provision;

1.4. Act CXX of 2001 on the capital market;

1.5. Act CXXXVIII of 2007 on investment companies and commodity exchange service providers, and on the rules of their activities;

1.6. Act LXXXV of 2009 on the Pursuit of the Business of Payment Services;

1.7. Act CXXXIX of 2013 on the Magyar Nemzeti Bank;

1.8. Act CCXXXV of 2013 on certain payment service providers;

1.9. Act CCXXXVII of 2013 on credit institutions and financial enterprises;

1.10. Act XVI of 2014 on collective investment forms and the managers thereof;

1.11. Act LXXXVIII of 2014 on insurance activities;

1.12. 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;

1.13. Commission Delegated Regulation (EU) 2015/35 of 10 October 2014 supplementing Directive 2009/138/EC of the European Parliament and of the Council on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II);

1.14. Act LIV. of 2018 on the protection of business secrets.

2. Data protection and information security regulations

2.1. Act CXII of 2011 on informational self-determination and the freedom of information;

2.2. Act L of 2013 on electronic information security at state and municipal organisations and its implementing regulations;

2.3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR).

3. Recommendations and guidelines

3.1. Guidelines on outsourcing of the Committee of European Banking Supervisors of 14 December 2006;[16]

3.2. Guidelines on system of governance of the European Insurance and Occupational Pensions Authority (EIOPA-BoS-14/253)[17], and the related „Final Report on Public Consultation No. 14/017 on Guidelines on System of Governance");[18]

3.3. Recommendations on Cloud Outsourcing of the European Banking Authority (EBA/REC/2017/03);

3.4. Recommendation 15/2015 of the MNB on the safety of financial services provided online;

3.5. Recommendation 27/2018 (XII. 10.) of the MNB on internal defence lines and the governance and control functions of financial institutions;

3.6. Recommendation 4/2016 (VI. 6.) of the MNB on the governance system of insurers and reinsurers;

3.7. Recommendation 7/2017 (VII. 5.) of the MNB on the protection of information systems.

4 Acts on designating essential systems and facilities

4.1. Act CLXVI of 2012 on the identification, designation and protection of essential systems and facilities;

4.2. Government decree 330/2015 (XI. 10.) on the identification, designation and protection of essential systems and facilities in the financial sector.

[16] The Guidelines of the Committee of European Banking Supervisors are available on: https://www.eba.europa.eu/documents/10180/104404/GL02OutsourcingGuidelines.pdf.pdf

[17] EIOPA's guidelines are available on: https://eiopa.europa.eu/guidelinessii/eiopa_guidelines_on_system_of_governance_en.pdf

[18] EIOPA's report is available on: https://eiopa.europa.eu/publications/consultations/eiopa_eiopa-bos-14-253-final%20report_governance.pdf

Table of contents