PRUDENTIAL MODELLING AND INFORMATION TECHNOLOGY SUPERVISION DEPARTMENT

Frequently asked questions concerning the use of cloud services (FAQ)

TRANSLATION

1. Consultation

1.1. Is there an option for the Institutions to consult with the Supervision concerning the use of cloud services?

Yes, the Supervision is open for consultation, which should be initiated via the appointed supervisor of the institution or the home page of the IT Supervision[1]. In complex cases of innovative financial solutions which require the involvement of several supervisory areas, and in case of innovative solutions, for which the Fintech innovator does not hold a licence, MNB Innovation Hub (https://www.mnb.hu/innovation-hub) provides a platform to seek regulatory assistance. MNB Innovation Hub can be contacted through the questionnaire[2] available on the platform.

1.2. When is it reasonable to consult with the Supervision?

Consultation with the Supervision is not mandatory, but we advise the Institutions to consult with MNB before entering into cloud outsourcing with high impact, involving critical functions, or to ask for guidance before provisioning cloud services if necessary.

2. Regulation

2.1. What is the regulatory background for the use of cloud services?

Generally, for the financial sector, information security requirements are set out by Government Decree No. 42/2015. (III. 12.) on protecting the information system of financial institutions, insurance undertakings, reinsurance undertakings, investment firms and commodity dealers, as well as by sectoral laws.
Use of cloud services, specifically, is regulated (at the time this FAQ is published) by Recommendation 4/2019 (IV. 1.) of the Magyar Nemzeti Bank[3] on the usage of community and public cloud computing services (Cloud recommendation), Recommendation 8/2020. (VI.22.) of the Magyar Nemzeti Bank[4] on the security of information systems, EBA's [5] Guidelines on outsourcing arrangements (EBA/GL/2019/02), EIOPA's[6] Guidelines on outsourcing to cloud service providers (EIOPA-BoS-20-002), and ESMA's[7] guidelines on cloud outsourcing which are currently under preparation. Outsourcing is (currently) regulated by

[1] https://www.mnb.hu/felugyelet/szabalyozas/informatikai-felugyelet

[2] https://mnbpoll.mnb.hu/Survey.aspx?surveyid=70754442&lng=hu-HU

[3] English translation: https://www.mnb.hu/letoltes/4-2019-cloud-bg.pdf

[4] English translation: https://www.mnb.hu/letoltes/2020-on-the-protection-of-it-systems.pdf

[5] European Banking Authority

[6] European Insurance and Occupational Pensions Authority

[7] European Securities and Markets Authority

20.06.2022.

Recommendation 7/2020 (VI. 3.) of the Magyar Nemzeti Bank on the usage of external service providers. Other relevant legislation, recommendations and guidelines are referenced in the MNB Cloud recommendation.

3. Definitions

3.1. What factors determine whether a cloud service model qualifies as private or community cloud?

If the service provided fulfils the criteria of a cloud service, but the infrastructure is under the control of the Institution in its entirety, and the service is used exclusively by the Institution, it qualifies as a private cloud. If a cloud is used exclusively by a group of companies (e.g. members of a corporate group), it constitutes a community cloud. In case a group of companies uses a public cloud service together, that constitutes as public cloud.

3.2. What is a private cloud?

The principal quality of a private cloud is that every constituting IT equipment and software is under the sole control of the organisation using it, therefore the Institution bears all responsibility concerning its hardware, software, infrastructure, and availability. These resources are not shared with outside participants, they are only accessible from inside the organisation.

3.3. Is managed private cloud considered as private cloud?

As a general rule, no. The MNB Cloud recommendation contains no reference to managed private cloud, the definition and usage of the term is inconsistent and contradictory across the industry. According to a popular definition, a managed private cloud uses the client's data centres and devices, but the operation and maintenance of the cloud infrastructure is the task of a service provider. According to another interpretation the managed private cloud service provider operates their own cloud infrastructure and provides the service on devices which are made exclusively available to the customer. According to the MNB's interpretation, a cloud service can only be considered as private cloud if the infrastructure supporting the service provided to the Institution is segregated on a hardware level. Even in the case of such an arrangement, outsourcing regulations should be observed.

3.4. Is a cloud service used exclusively by the members of a group considered as private cloud?

No, such an arrangement is a community cloud. For further explanation, see Question 3.1.

4. Scope of the cloud recommendation

4.1. Is the MNB Cloud recommendation applicable to insurance agents?

If the agent's activity encompasses the processing of client data– including the data belonging to the agent's clients – by using cloud services, it is in the recommendation's scope. The Cloud recommendation shall be taken into consideration in those cases as well when the usage of the cloud services is not based on an outsourcing agreement.

5. Compliance

5.1. If a cloud service is compliant with EBA/EIOPA/ESMA requirements, is compliance with MNB's cloud recommendation also required?

The MNB Cloud recommendation contains the requirements set out in the EBA/EIOPA/ESMA guidelines but determines further information security requirements for the entire life cycle of the service, by also taking the Hungarian legal environment into account. Therefore, compliance with MNB's cloud recommendation is also necessary.

5.2. Which cloud service models, solutions or service providers are accepted by the Supervision?

The Supervision sets out its requirements in a supplier and technology neutral manner, since the Supervision focuses on robust data protection, transparency, the proper management of arising risks, the adequacy of control measures and legal compliance regarding the use of cloud services.

5.3. Is MNB Recommendation No. 4/2019 (IV. 1.) on the usage of community and public cloud computing services applicable to temporarily used cloud services?

The MNB Cloud recommendation should also be applied to cloud services which the Institution procures for a limited amount of time (e.g. cloud bursting). For such services, the entire life cycle of cloud services applies, therefore the requirements set out in the MNB Cloud recommendations should be complied with (including recommendations on entering the details of the arrangement into a register and the reporting the contract to MNB).

5.4. Are Institutions which are registered as service providers required to provide information to the National Cyber Security Center also expected to comply with the MNB Cloud recommendation if they use cloud services?

Yes, provided that the Institution, organisation, person, or activity falls under any of the Acts set out in Section 39 of Act CXXXIX of 2013 on the Magyar Nemzeti Bank.

5.5. Which services are allowed to be outsourced into the cloud?

The services that may be outsourced are governed by sectoral laws, and by the MNB recommendation No. 27/2018. (XII.10.) on setting up and using internal lines of defence and on the governance and control functions of financial organisations, and MNB recommendation No. 7/2020. (VI. 3.) on the usage of external service providers. In general, services that may be outsourced may also be outsourced into the cloud, provided that risks are appropriately managed throughout the process. The MNB Cloud recommendation also applies if an outsourced service provider uses cloud services as a subcontractor while fulfilling their contract.

5.6. Which risk analysis methods are accepted by MNB for using cloud services?

The MNB does not favour any particular risk analysis methodology, but the risk analysis should demonstrably be able to fulfil the requirements of applicable sectoral laws, and the requirements determined by Recommendation No. 7/2017 (VII. 5.) of the Magyar Nemzeti Bank on the security of information systems.

5.7. What considerations should be taken into account when developing contractual requirements?

The contract should cover the entire life cycle of the service and all risks that may arise during that period. The pro forma contracts offered by the cloud service provider (CSP) may not be flexible enough to accommodate the Institution's requirements and achieve compliance with the regulatory environment. Therefore, it is recommended that the Institutions opt for the service package offered to financial institutions. Concerning important terms of contract, at least the following should be covered:

- conditions of termination, determining the termination period,
- unconditional audit rights,
- data processing and handling locations,
- data security and data protection requirements throughout the entire service chain,
- security requirements of processes and systems,
- incident management and fraud investigation (forensic) processes, and
- exit strategy.

Contractual requirements are governed in detail by the MNB Cloud recommendation, but sectoral laws governing outsourcing also apply, along with the cloud guidelines published by the European Supervisory Authorities.

5.8. What is considered best practice for the level of detail and documentation of the exit strategy?

Both an exit strategy and an exit plan should be developed. The exit strategy should contain the conditions of initiating an exit procedure, the timeframe of the execution, and the main steps and people responsible should be set out. It should contain the source, the channel, the tools, and the structure of the Institution's data to recoup, and it should cover the way the service will be provided after the termination of the contract (on-premise, different service provider). Exit plans should also cover the scenario of an unplanned exit. Terms and cost of exit should also be governed by the contract.

6. Information security

6.1. Is the redundancy provided by a single data centre adequate for the use of cloud services?

The redundancy provided by a single data centre is not enough, since it does not address major risks which potentially result in the loss of that data centre (i.e. natural disasters), the loss of internet connectivity to a certain region, or a blackout. Backups should also be stored in a different location which is not likely to be affected by the risks of the primary site, therefore the use of a single data centre is not adequate. See also paragraph 11.2.7. of the MNB Recommendation 8/2020 (VI.22.).

6.2. Is CSP independent backup necessary in every case?

Backups stored independently from the CSP[8] should be ensured based on the criticality of the functions and data, while taking relevant risks into consideration. The Institution should determine in detail whether an independent backup is necessary, and define the data that should be included, the frequency and method of creating backups, and where and how backup data should be stored. CSP independent backup can be implemented on-premise by the Institution or through a different CSP – but in the latter case, the storage of backups also falls under the purview of the MNB Cloud recommendation. Independent backups should also be ensured while using Software as a Service (SaaS) or similar, CSP specific services – in a risk proportionate manner – which should enable the Institution to restore the service as required by the business continuity plans and the exit strategy. The feasibility of CSP independent backup should be assessed during the preliminary analysis, considering the materiality of the service.

[8] such backups that are prepared and stored independently from the primary cloud service provider

7. Accountability

7.1. What duties does the Institution have concerning the tasks performed by the CSP?

CSPs contractually agree to offer certain service elements based on the service model (e.g. Infrastructure as a Service, Platform as a Service, Software as a Service). Institutions should, prior to signing the contract, analyse the risks attached to each cloud service element, assess the controls implemented by the CSP, and should make a documented decision about the Institutions' requirements which need to be met before the Institution deems the risks of a service acceptable. Naturally, if the risks cannot be mitigated adequately, signing the contract is not advised.
The Institution should periodically assess whether the CSP is performing its tasks in an adequate manner, and whether the operational risks presented by running the services in the cloud require corrective actions or the amendment or termination of the contract. If a major incident occurs, an unscheduled assessment should be performed.
For other service elements (e.g. user administration), CSPs only offer the possibility to ensure the security of the service, but the actual settings, administration should be performed by the Institution.
The separation of tasks should be defined in the contract. Responsibility and accountability for both the service offered to clients, and the protection of clients' data and assets, remain with the Institution – even if they choose to opt for using a cloud service.

8. Data protection

8.1. Is the inclusion of a CSP residing outside the European Economic Area acceptable?

Institutions should comply with the sectoral legislation and recommendations – but besides those, legal requirements for data protection (e.g. EU General Data Protection Regulation) and information security should also be met. If the usage of a cloud service involves a country which is either not an EEA[9] member state or a country which does not have data protection equivalent to the EU's, the Institution should be able to provide sufficient information to the relevant authorities about both the risks arising from such an outsourcing and the methods of risk mitigation. Therefore, moving data to a location outside the EEA creates additional assessment and control requirements, which should be enforced through contractual and technological means.

9. Auditing cloud services

9.1. What are the requirements for accepting third party audit reports and certifications concerning cloud services?

Reports and certifications issued by third parties which are legally independent from the Institution should provide assurance on the existence and the effective operating of controls; their scope should cover the service in its entirety (timescale, processing locations, controls, services, systems, etc.). The personnel conducting the audit/certification should possess relevant skills which satisfy the requirements of the Institution. The Institution should have the right to inspect relevant audit findings and evidence and should be able to interpret the findings and recommendation within its own risk management framework. Potential findings and recommendations should be rectified in a documented manner. Multiple clients may conduct joint audits at the CSP. CSPs are not supervised or evaluated by the Supervision, but the Supervision reserves the right to conduct an audit of outsourcing at the CSP if necessary. If the procurement of the cloud service

[9] European Economic Area

qualifies as outsourcing, the audit requirements for outsourcing arrangements set out by sectoral laws should also be adhered to.

9.2. To what extent does the Supervision accept independent audit reports or certifications in the context of cloud services?

The Central Bank of Hungary (MNB) may take third party audit reports into account at its own discretion, depending on their scope, level of detail, reliability, and level of independence. The audit processes of the Institution should set out the conditions based on which the Institution accepts third party reports and certifications, and it should be able to demonstrate that the reports accepted by the Institution satisfy these conditions, and comply with legal and regulatory requirements.

10. Qualifying as a cloud service, reporting and reporting obligations

10.1. Is it considered a cloud service if, in the case of an outsourced service, the virtualization layer, the operating system and the application are operated by the institution, but the storage is operated by the service provider, and customer data are separated at the storage level (different volumes per customer); but the storage is the same?

This allocation is not considered a standard cloud model[10], it can be considered almost pure hardware hosting (which is not a cloud service). If the institution has no control over storage and volume management and cannot manage resources in a self-service manner, in a dynamic way, then the service should be treated as an outsourcing.
However, if the criteria of cloud service are met[11], the service should be considered as a cloud service and should be evaluated accordingly, based on the outsourcing requirements and the Cloud recommendation, and the institution shall gain assurance that the service provider handles the storage, configuration and separation properly.

10.2. Is it necessary to report applications that support video conferencing (Zoom, MS Teams)? If, say, (only) the institution's service provider / partners (i.e. not customers) are contacted, should this be reported to the MNB (e.g. in the frame of quarterly data provision)?

Institutions are obliged to fully report the cloud services used, with the aim of ensuring that institutions use cloud services only in a sufficiently transparent and controlled manner, excluding the unsafe use of cloud services such as so-called “shadow IT”. It is important that the Cloud Recommendation requires that a risk analysis be carried out for the cloud services used, and based on the results, it is necessary to apply the additional measures expected by the Cloud Recommendation in accordance with the risks. For expectations regarding the security of applications that support video conferencing, see section “VII.4. Fax, telephone, conference, video conferencing calls, and other communication channels” of the Recommendation 12/2020. (XI.6.) of the Magyar Nemzeti Bank on the information security requirements of teleworking and remote access[12]. Regarding the requirements ensuring the legitimacy of the software tools used, see section

[10] In the case of Infrastructure as a Service (IaaS), the underlying cloud infrastructure is not managed by the client but may have/has control over the storage.
[11] See paragraph 1. of the Cloud Recommendation:
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 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).
[12] https://www.mnb.hu/letoltes/12-2020-recommendation-of-teleworking.pdf

"5.3. Agreements proving the legitimacy of installed software" of the Recommendation (currently) 8/2020. (VI.22.) of the Magyar Nemzeti Bank.

10.3. In the case of a group of financial undertakings, is it necessary to report the jointly used internal network and other on-premise services (e.g. file server, AD, correspondence) as a cloud service?

It is necessary to report these services as cloud services if the jointly used services are implemented by using cloud services. In this case, the MNB expects all group members under its supervision to report it. If the services used jointly are not implemented by using a cloud service, but are considered outsourcing, they should be reported as intra-group outsourcing.

10.4. What exactly should the institution report as part of the quarterly reporting obligation?

As provided for in Article 4, paragraph (1) of the MNB decree in force of the Governor of the Magyar Nemzeti Bank on the data reporting obligations to be fulfilled by financial and credit market institutions to the central bank information system primarily for the purpose of performing the supervisory tasks of the Magyar Nemzeti Bank:[13] "The credit institution and the credit institution type EEA branch shall – with the exception of paragraph (2) – submit a supervisory report to the MNB with the content, form, frequency and deadline as set out in Annex 2."
The data content currently required:

- cloud service provider's name;
- cloud service provider's headquarters;
- cloud service provider's tax number;
- the name of the parent company of the cloud service provider;
- the headquarters of the parent company of the cloud service provider;
- the tax number of the parent company of the cloud service provider;
- activities and data and data categories affected by the use of cloud services;
- the country or countries in which the service is provided (including the location of handling, processing and storing of data);
- the commencement date of the service;
- the date of the contract in force;
- the next contract renewal date (where applicable);
- the applicable law governing the contract.

The above data must be filled in for each cloud service by repeating the relevant lines, on the sector data reporting worksheets (Credit Institutions: 9I; Financial undertakings: 29IT; Payment institutions: 86I; Insurers: 42Q23; Investment firms: 37G, Fund Managers: 50U; Funds: 71OPI,71EPI, 71MPI,76NPI). All data reports come with a fill-in guide, which consistently includes the following for the cloud service (e.g. for 9I): The definition of "cloud service" in line 9I11 and the explanation of the information requested in the lines containing the details of line 9I11 are contained in the Recommendation 4/2019 (IV. 1.) of the Magyar Nemzeti Bank on the usage of community and public cloud computing services. In case the institution uses several cloud services, the answers must be provided by filling in multiple blocks.

[13] currently Government Decree No. 55/2021. (XI. 23.): https://www.mnb.hu/statisztika/informaciok-adatszolgaltatoknak/rendeletek-allasfoglalasok/55-2021-xi-23-mnb-rendelet

11. Documenting the cloud service

11.1. What documentation do we need for cloud service? (These are requested by the MNB during a supervisory examination)

Paragraph 62. of the Recommendation 4/2019 (IV.1.) of the Magyar Nemzeti Bank on the usage of community and public cloud computing services (hereinafter referred to as the "Cloud Recommendation") summarises the most important documentation requirements, which are the following currently:
"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."

Additional documentation requirements are laid down in paragraphs 16. and 29. of the Cloud Recommendation in relation to the assessment and decision-making of outsourcing, and the register.

11.2. If a group of companies had already used a community cloud service in the past (before 2017), is it necessary to prepare all the documents required by the Cloud Recommendation afterwards? Furthermore, in connection with testing and piloting, what documentation and notification obligations does the institution have?

Of the documents required by the Cloud Recommendation, only the document necessary for the decision to use the cloud service, the pro-con analysis, does not need to be prepared afterwards. Apart from this, it is necessary and appropriate to prepare the documents requested in the Cloud Recommendation afterwards. Paragraph 62. of the Cloud Recommendation summarises the most important documentation requirements, which are currently as follows:
"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."

Some requirements which are also applicable after the implementation (e.g. risk analysis, evaluation of controls, examination and development of contract compliance, see above) must be carried out during the risk analysis.
The EU's sectoral supervisory authorities also expect compliance with their guidelines for cloud services already being used – the EBA by 31 December 2021, EIOPA and ESMA by 31 December 2022 – however it is not necessary to prepare the documents necessary only for the decision making on the use of cloud service.
In connection with testing and piloting, the institution has no documentation or reporting obligations, provided that they do not use sensitive data (trade secrets, financial sector secrets, personal data) or

support production processes. In the case of the use of sensitive data or production processes, the provisions of the Cloud Recommendation shall be fully applied. For detailed requirements on testing, see paragraph 4.4.8. of the Recommendation (currently) 8/2020. (VI.22.) of the Magyar Nemzeti Bank on the security of information systems.[14]
Additionally, the MNB evaluates compliance with the applicable laws and recommendations during the examinations.

11.3. In the case of a group of companies comprising financial undertakings using community cloud services, what options are available to simplify the risk analysis expected of individual group members (e.g. is it sufficient for the group members to use the risk analysis for the service provider, supplemented by their own risks)?

The Institution may rely on the group level risk analysis if its scope and quality are aapropriate, but it must supplement the risk assessment with its own risks, their assessment and, in doing so, taking into account local legal requirements.

11.4. What level of risk and frequency of occurrence shall be associated with the event that the service provider makes a sudden decision to suspend the provision of the service to a region or country?

Risk analysis is the institution's competence to assess its own risk tolerance, as well as the possibilities and time required for relocating the service.
The risk analysis should also cover geopolitical risks associated with the cloud service provider. In case geopolitical risks may increase to an unacceptable level, it may render the risk-proportionate implementation of the cloud services unfeasible or may jeopardise the orderly exit of the service by not providing the possibility of moving the service or the time required to carry it out.

11.5. What are the MNB's minimum requirements for the content of the contract? In the case of cloud services providing collaboration services, what contractual additions/solutions can be applied, what should be paid special attention to?

The financial services contracts typically contain the mandatory content elements, however it is the responsibility of the Institution to verify compliance with sectoral legislation and the recommendations of the MNB prior to the conclusion of the contract. For further details, see paragraph 25. of the Cloud Recommendation.

12. Auditing cloud services

12.1. What evidence and specific access should the institution have in order to gain assurance on, for example, the adequacy of the encryption carried out by the service provider and the security log analysis guaranteed 0-24 hours?

Verifying compliance may be carried out through the management interface of the devices providing the service, and in the case of security log analysis, by documents (e.g. screenshots) extracted from the Security Information and Event Management (SIEM) system, that demonstrate the receipt of the relevant log files in the SIEM, as well as security log analysis reports or extracts prepared from them, filtered for the institution.
In addition, the Institution may rely on its own or third-party compliance and audit reports and certificates.
If the Institution uses self-generated encryption keys, it can obtain further assurance on the proper

[14] 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.

functioning of the controls (e.g. BYO key, HSM module). For further details on this matter, see also section III.2.3. Assurance of the Cloud Recommendation.

12.2. How frequent penetration testing does the Supervision recommend for cloud services?

The contract must be taken into consideration, and more specifically we propose a risk-proportionate approach. In this regard, the MNB's document on Frequently Asked Questions and Answers in relation to the conduct of vulnerability tests and penetration tests (FAQ) provides guidance[15], and according to paragraph 10.: “According to Section 13.1.4. point f) of the 8/2020. (VI.22.) MNB Recommendation: "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;" (...) It is recommended to conduct a penetration test also on systems which are not accessible from the internet but process critical data (see Section 4.4.8. of 8/2020. (VI.22.) MNB Recommendation)”.

12.3. According to section III.3. Contractual requirements, paragraph 25. point (e) of the Cloud Recommendation: “contractually defined and stipulated (…)

e) If relevant to the entity, the right to certify the services provided by the CSP based on Government Decree 42/2015 (III. 12.)”. Is this requirement satisfied if the contract with the service provider stipulates that the service provider must submit to the certification of the service according to Government Decree 42/2015. (III. 12.), if the service undergoes a certification by the certification body?

The consent to submit to general audit also includes the possibility of conducting a secure information system audit.

13. IT activities related to cloud services

13.1. When using cloud services, what are the specific planning and day-to-day operations tasks of IT development and operations (operational safety, DR capability, etc.)?

The tasks depend on the service model used, for example, it depends on whether the institution only configures the permissions, password parameters in a system, and everything else is operated by the service provider, or the service provider only provides and operates the platform, and the rest is managed by the institution. The operating and the DR capabilities of the devices, systems and functions remaining in its own management must be provided by the Institution. When concluding a contract, the allocation of responsibilities must be clearly set, and DR procedures, their cost implications and the notification chain should be clarified with the cloud service provider.

13.2. In what form does the MNB expect the DLP, SSL inspection (mandatory?) requirements set out in the MNB recommendation 8/2020 to be implemented, e.g. in the case of an institution using a SaaS service?

Data leakage prevention requirements should also be examined for a SaaS service and enforced in proportion to the risks for the entire data lifecycle (storage, sharing, use, etc.) in all possible data leakage channels. It is necessary to assess in advance what data security controls are available (service provider DLP, encryption, anonymization, etc.) and to take this into account and evaluate it when analysing the risks of

[15] https://www.mnb.hu/letoltes/penteszt-faq-v1-final.pdf
For more detailed instructions, see the website of the MNB's Information Technology Supervision Department: https://www.mnb.hu/felugyelet/szabalyozas/informatikai-felugyelet

cloud service, selecting or discarding the cloud service. Decryption and inspection of encrypted channels in proportion to risks (e.g. with netbank channels as an exception) or, failing that, the use of compensatory controls (for example, blocking categories that could be leaked or that pose a security risk and uncategorized pages on a WEB content filtering channel) is required for both cloud and non-cloud implementations.

14. Cloud service management aspects

14.1. What is the MNB's position on the handling of bank secrets in the cloud service?

The MNB expects the implementation and the operating of risk-proportionate controls, and if these exist, bank secrets can also be managed in cloud service. For more information, see the privacy requirements of the Cloud Recommendation:

1. section III.1.1. Ensuring legal compliance of cloud services, paragraph 9.;
2. section III.2.1. Location of data and data handling;
3. section IV.1. Data security, data and confidentiality;
4. Annex 1, section 2: Data protection, data and secrecy protection.

14.2. As a system integrator or bank supplier, is it possible to consult with the MNB, if so, what is its exact course?

The MNB holds consultations mainly with the supervised institutions but is open to consultation with other companies depending on the available capacity. The supervised institutions may indicate their request for consultation to the supervisor of the institution, or in case of a specific question we recommend that they contact the MNB's IT Supervision Department at the home page of the IT Supervision[16] or iff@mnb.hu e-mail address.

14.3. When will the new version of Recommendation 4/2019 be released and with what number?

We do not consider it appropriate to review the content of the recommendation until the DORA regulation is published.

[16] https://www.mnb.hu/felugyelet/szabalyozas/informatikai-felugyelet

Table of contents