KPMG

Financial Risk&Regulation

MNB published a new AML recommendation, and it also supplemented the recommendation of the internal line of defense

Newsletter – October 2022

A recommendation addressed to financial organisations has been published by National Bank of Hungary (MNB), which provides guidance on the assessment of money laundering and terrorism financing risks and the definition of related measures, replacing the previous MNB recommendation. The MNB expects the recommendation to be applied from January 1, 2023 and in addition to this, MNB also recently published the revision of its recommendation on the Internal Lines of Defense for financial institutions, in which it amended the regulation issued in 2018 in several places. Similar to the previous version, the recommendation sets expectations for the layout of internal defense and its operation, except for a few points of the new recommendation, which will enter into force on January 1, 2023. The main changes of the recommendation affect three different topics, on the one hand, the prevention of money laundering and terrorism financing, on the other hand, the establishment of an internal audit trail, and employer training on internal lines of defense.

AML/CTF recommendation

The publication of the new recommendation is justified by the change in the legal environment governing the European Union, in particular the revision of the EBA Guidelines, which are the basis of the previous recommendation on risk factors related to money laundering and terrorism financing published by the European Banking Authority on March 1, 2021. Compared to the previous recommendation, in Hungarian context the 26/2020. (VIII. 25.) MNB decree is considered a new element. The above mentioned regulations and Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing have been taken into account for this publication, which is intended to share the expectations and best practices regarding new types of AML/CFT risks with service providers. The recommendation consists of two main parts: a comprehensive regulatory part and, for the most part, a sector, activity-specific part.

The following stakeholders are affected by the recommendation:

- credit institutions,
- financial service providers,
- occupational pension providers,
- voluntary mutual insurance funds
- those who collect and deliver international postal orders,
- fiduciary trustees.

For occupational pension providers, voluntary mutual insurance funds, those performing international postal order acceptance and delivery, as well as fiduciary trustees, the supervisory organization only expects what is written in the chapter concerning the general principles of risk assessment and management of the recommendation. Emphasizing the role of

internal risk assessment and formulating related expectations is almost a central element that spans the entire material. The MNB expects service providers to categorize their business lines in their risk assessment; their business relationships and transaction orders. As part of this, the service provider must have a **comprehensive picture** of the ML/TF (money laundering/terrorism financing) risk factors it has uncovered, and must use these to assess the general level of ML/TF risk. The service provider may decide to weight individual risk factors differently depending on their relative importance.

The recommendation suggests the service provider to apply a comprehensive and unified approach to the risk associated with the situation, and it is recommended to take into account that, unless the legislation provides otherwise, **isolated risk factors do not necessarily classify the business relationship into a higher or lower risk category**. When weighing the risk factors, the service providers are recommended to evaluate with sufficient information the relevance of the various risk factors related to the business relationship and the transaction order. The recommendation offers the following example of these relationships: the service provider may assign different risk values to different factors for the reason that the client's personal relationship with a country presenting a higher ML/TF risk is less relevant in view of the characteristics of the product he is looking for. Deciding on the most appropriate way of risk categorization remains the service provider's responsibility.

A new term also appears in the recommendation, the **dynamic customer due diligence**: MNB expects the service providers to use information obtained during the existence of the business relationship for risk assessment purposes. In addition, gather sufficient information about their prospective clients to ensure that they have disclosed all relevant risk factors at the start of the business relationship, during the existence of the business relationship and before the execution of the transaction order. The use of the list specified in Annexes 1 and 2 of the Regulation of the Minister of National Economy (12/2017. (VIII. 3.) is also mentioned.

In the field of customer risk factors, a new risk element is when the customer's account only receives credits from accounts held abroad and transfers are only made to accounts held abroad; domestic transactions are in small amounts and typically the costs necessary for the establishment and operation of the company (e.g. lawyer, bookkeeping services, registered office service), and **the customer does not carry out any actual economic activity in Hungary**. The MNB describes that in such cases **it is necessary to examine the rational economic reason for which the customer chose to open an account in Hungary**.

The call to attention for increased terrorism financing risks is also a new element of the publication, highlighting cases such as when the client is a non-profit organization whose operations or leadership are known to be sympathetic to extremism or terrorism. The recommendation suggests special attention to the typology of the Financial Action Task Force (FATF) in the related topic.

The supervision also expects that the service provider's policies and procedures for the prevention of money laundering and terrorism financing are based on its risk assessment, and makes specific proposals for them. Among other things, what counts as a transaction order, the level of customer due diligence and the risk appetite of the service provider must be determined.

An interesting element of the recommendation is **the issue of de-risking**, according to which an institution will no longer provide services to certain customer categories presenting a high ML/TF risk. The MNB emphasizes that service providers must apply appropriate and risk-sensitive policies and procedures during their effective customer due diligence, and therefore unjustified denial of access to financial services for an entire customer base is not acceptable. In other words, the recommendation expects the service providers to carefully balance the need for financial integration and the need to reduce ML/TF risk through de-risking. The recommendation specifically refers to the EBA opinion on the application of customer due diligence measures to asylum-seeking customers from higher-risk third countries or territories.

In addition to the above, **the Supervisory Authority formulated modified or minor new expectations in connection with other customer due diligence measures**. Examples include: proof of identity, risk-based evaluation of politically exposed persons, definition of high-risk situations, and rules for the use of innovative technological tools for checking the customer's identity.

The second main part of the recommendation consists of the **detailed sector-specific guidelines**, where, in addition to "traditional" financial organizations, there are special expectations for institutions providing correspondent banking services, as well as sector guidelines for institutions providing remittance services and asset management services. These last three sector guidelines have changed compared to the previous recommendation, and new sector-specific guidelines have also been included:

- customers offering services related to virtual means of payment;
- sectoral guidelines for service providers providing payment initiation services and account information services;
- sectoral guidelines for service providers performing currency exchange activities;
- sectoral guidelines for corporate financing..

Based on the content of the recommendation and its interpretation, it can be seen that the Authority wishes to achieve stronger preventive controls, awareness of a risk-sensitive approach, and thus emphasize the importance of prevention. The increasingly detailed risk-based supervision expectations can also help in the development and improvement of typical shortcomings, such as bad reporting practices, inadequately parameterized filter systems, or poor documentation practices of the logic underlying the scenarios used for screening. In the past, both domestic and foreign supervisors have imposed significant penalties on institutions that manage financial crime risks improperly, so it is particularly important to handle these topics carefully and thoroughly.

Internal lines of Defense recommendation

The MNB has harmonized Hungarian expectations with European-level guidelines. The recommendation transposes the European Banking Authority's (EBA) guidelines on internal governance published on July 2, 2021, in addition to the MiFID II directive, published by the European Securities and Markets Authority (ESMA) on April 6, 2021 on certain aspects of the requirements for the compliance function according to the directive, as well as some provisions of the joint guidelines of EBA and ESMA on the assessment of the suitability of senior board members and persons performing key services published at the same time.

In the updated recommendation, the financial organizations' three-level internal line of defense has been specified, which is made up of the responsible internal, as well as the supplementing controls built into business processes of the second and third lines of defense that complement the controls built into the business processes.

The MNB emphasizes in the update that the size and systemic importance of the financial organization are not in themselves related to the degree of exposure to risk.

The MNB expects the relevant financial organizations to apply the recommendation - with the exception of what is contained in the section on the designation of the person responsible in connection with the prevention of money laundering and terrorism financing - from January 1, 2023. The assignment of potential board members of the issued recommendation is applicable from January 1, 2024. On January 1, 2023, the former 2018 MNB recommendation on the establishment and operation of internal defense lines and the management and control functions of financial organizations will expire (27/2018 (XII. 10.)).

The new recommendation places greater emphasis on money laundering and terrorism financing, as well as the prevention of fraud

The „responsible internal governance" chapter has been expanded with paragraphs on the prevention of money laundering and terrorist financing, as well as the topic of fraud prevention and management.

The MNB expects financial organizations to develop processes and procedures in order to fulfil their obligations related to anti-money laundering and terrorism financing. Accordingly, it will be necessary to regularly evaluate the exposure of the financial organization to the risk affecting the topic, and if necessary, take steps to mitigate the risks. In this recommendation, MNB also emphasizes that a risk-mitigating step can be the training of employees related to the risks of money laundering and terrorism financing.

In parallel with the above, financial organizations will be expected to assign a member of the governing body who will be responsible for complying with the requirements related to the prevention of money laundering and terrorism financing. If there is no governing body, in that case a member of the organization's executive management is expected to be assigned to the position.

With regard to fraud, MNB emphasized that it expects the financial organizations to develop a fraud prevention and management culture that strives for zero tolerance for fraud and primarily focuses on fraud prevention. There are many possible solutions for this, the effective application of which is particularly important due to the deterioration of the risk environment.

For larger, more complex financial institutions - including credit institutions with a market share exceeding five percent of the total balance sheet - MNB expects institutions to appoint a chief officer (CRO) who performs a management function in terms of operational risk management and risk control function.

The Supervisory Authority formulated more detailed expectations regarding the internal management system

In addition to the section on money laundering, the „responsible internal governance" chapter has also been expanded to include a three-part section on control systems.

It is necessary for the financial organizations to establish and operate the control system and control trail documented in its internal regulations, which helps to identify risks. This comprehensive register has not yet been implemented in many institutions, so it is worth allocating adequate time to create it:

Based on the expectations of the Supervisory Authority, audit trails include:

- processes and activities set in place at the financial organization;
- the position responsible for managing the activities;
- role name;
- the legal basis for the provision of processes and activities;
- the process and task descriptions.

In-process control:

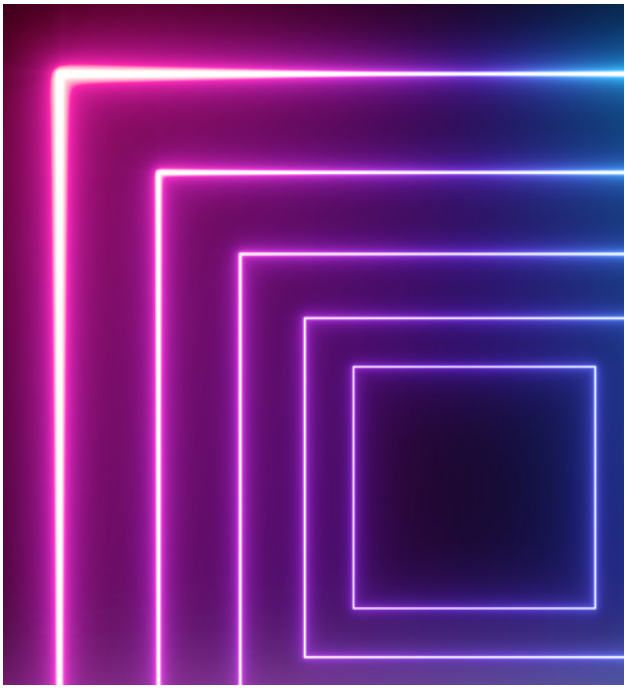
The MNB expects financial organizations to design their individual business processes and internal regulations in such a way as to enable control built into the process. It is necessary to include control stages in each process, the same person cannot be responsible for performing, processing and reviewing a given operation (separation of duties at an appropriate level/ principle of four eyes).

Management control:

Validation of management control functions at all management levels is expected. The purpose of the expectation is that the managers of the organization regularly check and report to subordinates in accordance with the internal regulations.

Management information system:

The MNB expects the management information systems to be designed and operated in such a way that it supports the activities of the financial organization's management with the available information. Primarily, the use of electronic devices and channels is recommended for the operation of management information systems.



Knowledge of the management system must be made known to all employees

In the new recommendation, the list of tools for managing personal conflict has been expanded. Regular education and awareness-raising campaigns regarding situations, practices, and transactions resulting in conflicts of interest as stipulated in the internal regulations.

This is related to the fact that, in its new recommendation, the Authority formulated several new detailed regulations in order to prevent conflicts of interest, in which it is important to inform the parties concerned. One such change, for example, is that in addition to the employees, the economic conflict of interest due to their close relatives has also been named.

The initiation and maintenance of these measures is achieved through workplace awareness of internal rules and internal-external communication, but the greater emphasis is on education and knowledge transfer. In addition to the fact that from now on financial organizations must train not only permanent employees, but also newly hired employees in fraud prevention and control, it is advisable and recommended to repeat the training every year. The financial organizations are expected to put together a training and education system tailored to organizational units, groups, and jobs, with which the greatest possible degree of efficiency can be achieved. Within the framework of the program, employees can familiarize themselves with the main characteristics of typical fraud events, the practices of deception, and the methods used and developed for their recognition and treatment.

Education must also be part of the financial organizations' or groups' strategies, policies, internal regulations, internal procedures and rules of procedure, so that the employees get to know and understand the financial organization's or groups' strategies, policies, internal procedures and rules of procedure to the extent appropriate to their work and level of responsibility, and to be informed about their changes continuously and at the appropriate time.

The adequacy of the internal management system is an important control function for the stakeholders of the financial sector in a particularly difficult economic situation, so its review may not only be relevant for the financial sector because of the new MNB recommendation. In addition to the appropriate training and education of employees on the subject, the new money laundering and fraud prevention rules can also be a challenge for the stakeholders. In this regard, it is important to review the current control framework and expand it with effective controls, not only due to the authorities' expectations, but also to reduce the risks that may cause financial loss.

The newsletter was prepared by: Dániel Bernáth, Gergő Wieder, Péter Vajda and Selima Kihal

Contacts:

Ágnes Rakó
Partner
M: +36 70 370 1792
E: agnes.rako@kpmg.hu

Péter Szalai
Associate Partner
M: +36 70 370 1739
E: peter.szalai@kpmg.hu

Gergő Wieder
Director
M: +36 70 333 1471
E: gergo.wieder@kpmg.hu

József Soltész
Senior Manager
M: +36 70 370 1766
E: jozsef.soltesz@kpmg.hu

Dániel Bernáth
Senior Advisor
M: +36 70 978 7049
E: daniel.bernath@kpmg.hu

KPMG.hu

BLOG