LIETUVOS BANKAS
EUROSISTEMA

OVERVIEW OF BUSINESS-WIDE ASSESSMENTS OF MONEY LAUNDERING AND TERRORIST FINANCING RISKS PERFORMED BY FINANCIAL MARKET PARTICIPANTS

Occasional Paper Series

No 36 / 2021

ISSN 2424-3213 (online)

Occasional Paper Series

No 36 / 2021

OVERVIEW OF BUSINESS-WIDE ASSESSMENTS OF MONEY LAUNDERING AND TERRORIST FINANCING RISKS PERFORMED BY FINANCIAL MARKET PARTICIPANTS

Drafted by:
Financial Market Supervision Service
Anti-Money Laundering Division
Contact details:
info@lb.lt.
+370 800 50 500

Gedimino pr. 6, LT-01103 Vilnius

www.lb.lt

The series is managed by the Applied Macroeconomic Research Division of the Economics Department and the Center for Excellence in Finance and Economic Research.

CONTENTS

EXECUTIVE SUMMARY

The Overview provides key insights into business-wide assessments of money laundering and terrorist financing risks performed by financial market participants. The Overview is based on conclusions obtained by the Bank of Lithuania from the supervision of financial market participants and on an analysis of risk assessments of 20 financial market participants (banks, electronic money institutions and payment institutions) and contains examples of good practice identified during the analysis and cases where risk assessments need to be improved.

1. OBJECTIVE AND METHODS OF THE OVERVIEW

When carrying out risk-based supervision and having regard to the fact that financial market participants (hereinafter – FMPs) have questions relating to the practical aspects of conducting business-wide assessments of money laundering and terrorist financing risks (hereinafter – risk assessment) of FMPs, in this Overview of Business-Wide Assessments of Money Laundering and Terrorist Financing Risks Performed by Financial Market Participants (hereinafter – the Overview) the Bank of Lithuania provides key insights into risk assessments performed by FMPs. The Overview is based on conclusions obtained by the Bank of Lithuania from the supervision of financial market participants and on an analysis of risk assessments of 20 FMPs (banks, electronic money institutions and payment institutions) submitted to the Bank of Lithuania for its supervisory functions.

The Overview is based on legal provisions and good practice and contains examples of good practice identified during the analysis of FMP risk assessments and cases where risk assessment needs to be improved.

2. OBJECTIVE OF RISK ASSESSMENT

Both international practice and the Republic of Lithuania legislation setting requirements for the prevention of money laundering and/or terrorist financing to be fulfilled by FMPs in order to prevent criminal activity very clearly stipulate that the process of assessing and managing money laundering and/or terrorist financing risks must follow a risk-based approach. Proper implementation of the risk-based approach is an essential part to establish processes for risk management and the prevention of money laundering and/or terrorist financing, starting with deep understanding of risks relevant to FMPs.

Article 29(1)(2) of the Republic of Lithuania Law on the prevention of money laundering and terrorist financing (hereinafter – the AML/CTF Law) sets out the requirement to establish adequate internal policies and internal control procedures relating to risk assessment and risk management as one of the key requirements in the area of managing money laundering and/or terrorist financing risks because only proper understanding and assessment of risks to which FMPs are exposed makes it possible to ensure in practice that measures taken to manage those risks are adequate and sufficient.

Risk assessment must not be formalistic and it's purpose must not only be to meet a legal requirement to conduct it but it must help FMPs to identify and understand money laundering and/or terrorist financing risks that FMPs may face when carrying out their activity and to take respective risk mitigation measures. Comprehensive risk assessment should help FMPs to understand what poses the highest money laundering and/or terrorist financing risk and in which areas of FMP activities the fight against money laundering and/or terrorist financing should be prioritised and what risk mitigation actions or measures FMPs should take. For instance, to carry out enhanced customer and beneficial owner due diligence, to implement enhanced ongoing monitoring procedures for business relationships and transactions, to update customer information more frequently, etc. FMP risk assessment should also help to prioritise and allocate FMP resources (IT, personnel, etc.) to areas where money laundering and/or terrorist financing risks are the highest.

It should be noted that risk assessment should correlate with the size and nature of the FMP's activity. FMPs only providing one type or limited services, for example, only payment initiation services or only utility payment services or other regular services to meet household needs, or services of collecting fines and/or other duties for public authorities and social benefit payment services might not need any complex and thorough risk assessment. However, FMPs whose activity size in terms of customer group, their geography, delivery channels and services or products offered is significant must undergo a risk assessment that is much broader and comprehensive in order to properly assess money laundering and/or terrorist financing risks to which such FMPs are exposed.

The main objectives of risk assessment are the following:

- to understand and assess money laundering and/or terrorist financing risks relevant for FMP
- to identify any gaps in the money laundering and/or terrorist financing risk management system and improve the risk management system
- to ensure that FMP management is informed and understands money laundering and/or terrorist financing risks to which the FMP is exposed in the course of their activities
- to help to make informed decisions on risks to be taken, the need for risk management measures and technologies and the allocation of human resources

3. GROUNDS FOR RISK ASSESSMENT

The importance of the risk-based approach for preventing money laundering and/or terrorist financing is emphasised in the Recommendations issued by the Financial Action Task Force for combating money laundering and terrorist financing (hereinafter – FATF), Directive (EU) 2018/843 of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (hereinafter – the Directive), the Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions approved by the European Banking Authority, the European Insurance and Occupational Pensions Authority and the European Securities and Markets Authority (hereinafter – the Risk Factors Guidelines) and legislation of the Republic of Lithuania.

- FATF Recommendations
  Directive
  Risk Factors Guidelines
- Law of the Republic of Lithuania on the Prevention of Money Laundering and Terrorist Financing
- Guidelines on the Prevention of Money Laundering and/or Terrorist Financing for Financial Market Participants

Article 29(1)(2) of the AML/CTF Law contains a provision on establishing adequate internal policies and internal control procedures relating to risk assessment and risk management. In accordance with Article 29(2) of the AML/CTF Law, such procedures must be established and risk assessment must be carried out taking into account at least customer risk, product, service and/or transaction risk, country-based and/or geographical area risk. Moreover, Article 29(3) of the AML/CTF Law stipulates what sources must be taken into account when developing internal control procedures including those relating to risk assessment and risk management. Article 29(7) of the AML/CTF Law stipulates that the management of FMP risks relating to money laun-

dering and/or terrorist financing must be an integral part of the common framework for risk management, and taking account of the size and nature of their activities, FMPs must put in place the procedures and frameworks intended for identification, assessment and management of the risk of money laundering and/or terrorist financing and effective risk-mitigating measures.

It should be noted that the obligation to have regard to the Risk Factors Guidelines is not only directly referred to in the AML/CTF Law but is also additionally emphasised in Decision No 241-174 of Director of the Financial Market Supervision Service of the Bank of Lithuania of 23 July 2018 on the application of the Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions approved by the European Banking Authority, the European Insurance and Occupational Pensions Authority and the European Securities and Markets Authority stating that FMPs should follow and respect the recommendations put forward in the Risk Factors Guidelines. Paragraph 10 of the Risk Factors Guidelines stipulates that firms' approach to assessing money laundering and/or terrorist financing risks associated with business relationships and occasional transactions should include business-wide risk assessments.

It should be noted that the Guidelines on the Prevention of Money Laundering and/or Terrorist Financing for Financial Market Participants approved by Resolution No 03-17 of the Board of the Bank of Lithuania of 12 February 2015 approving the guidelines on the prevention of money laundering and/or terrorist financing for financial market participants (recast of 1 March 2020) (hereinafter – the Guidelines) set out additional risk assessment requirements.

It should be noted that even though the legal requirement to carry out risk assessment has been in force since 2017, in the course of its risk-based supervision tasks the Bank of Lithuania has established that some FMPs have not performed such risk assessment in practice.

4. RISK ASSESSMENT

4.1. RISK ASSESSMENT PROCEDURE

REQUIREMENTS IN THE GUIDELINES
36. The FMP shall ensure that the procedure for carrying out the business-wide ML/TF risk assessment is adequately regulated and determines at least:
36.1. the sources of information used for carrying out the FMP's business-wide ML/TF risk assessment(s);
36.2. a data collection and evaluation procedure;
36.3. indicators identifying ML/TF risks, the likelihood of them emerging and their impact;
36.4. the duties and responsibilities of the staff member responsible for the FMP's business-wide ML/TF risk assessment;
36.5. a procedure for reporting the results of the FMP's business-wide ML/TF risk assessment to the FMP's management bodies;
36.6. the frequency of and a procedure for revising (updating) the FMP's business-wide ML/TF risk assessment;
36.7. a procedure for preparing and implementing an action plan for managing (mitigating) any risks identified.

Paragraph 36 of the Guidelines obliges FMPs to establish a risk assessment procedure and defines key aspects to be included in the procedure. It should be noted that proper identification and assessment of money laundering and/or terrorist financing risks to which FMPs are exposed with a view to ensuring that FMPs duly take adequate risk management/mitigation measures and performing risk assessment in practice become a difficult task for FMPs if they do not have a clear risk assessment process established, with its steps, staff duties and responsibilities and a procedure for using risk assessment results for further activities of the FMP. To ensure comprehensive and good-quality risk assessment, it is good practice to divide the risk assessment process into steps pertaining to planning, performance, result evaluation and the implementation of the action plan. The analysis of FMP risk assessments has shown that, when seeking to ensure that FMP staff responsibilities and duties are clearly distributed within the risk assessment process, the course of the risk assessment process is perceived uniformly and risk assessment results are comparable, some FMPs include in the procedure not only the information referred to in paragraph 36 of the Guidelines but also clearly and in detail establish risk assessment process and its course or steps.

It transpires from the analysis of FMP risk assessments that in their risk assessment procedures some FMPs have comprehensive, clear and structured methods/methodologies for identifying and assessing money laundering and/or terrorist financing risks making it clear how indicators identifying risks, the likelihood of them emerging and their impact and the final risk score are calculated, which is deemed good practice. It is recommended that a risk assessment methodology should be developed so that it is logical and objectively justified and that FMPs are able to explain and substantiate how money laundering and/or terrorist financing risks have been identified and assessed and how the controls established by the FMP for managing those risks have been assessed. Where in the course of risk assessment FMPs use mathematical models, it is recommended that the procedure for revising and amending such models also be established in a comprehensive manner.

To ensure that FMP risk assessment is in practice conducted in a comprehensive and thorough manner and that risk assessment methods employed by the FMP enable the FMP to identify and assess relevant money laundering and/or terrorist financing risks emerging in the FMP's activities, it is recommended to carry out regular assessment of methods for identifying and assessing money laundering and/or terrorist financing risks, to revise the FMP's risk assessment procedure and, if need be, to update it.

It should be noted that cases where the FMP's staff members are familiar with the risk assessment procedure and relevant amendments thereto are seen as good practice with a view to ensuring that the FMP staff members understand the risk assessment process, its steps and their own functions within the risk assessment process as well as the objective and importance of performing risk assessment in the course of the FMP's activities.

GOOD PRACTICE

1. The FMP has set risk assessment steps listing its business units that are responsible for the implementation of respective steps and their functions in assessing risks (e.g. from which business units (functions) information and data are collected and who is responsible for that, which staff members are responsible for structuring and processing data from various divisions, providing data analysis conclusions, identifying money laundering and/or terrorist financing risks in the respective area (e.g. customers, products, IT systems, etc.) and proposing to include them in risk assessment, finally evaluating all such information collected and validating it as well as coordinating the implementation of risk mitigation measures adopted after the assessment) and deadlines for submitting risk assessment results to FMP management.

2. The FMP risk assessment gives a brief description of the course and methods of risk assessment and contains links to the FMP's risk assessment procedure.

3. The risk assessment procedure describes methods for identifying and assessing money laundering and/or terrorist financing risks specifying how inherent money laundering and/or terrorist financing risks, the effectiveness of controls and residual risks are identified and assessed. Templates of crucial information needed for performing risk assessments are approved together with the risk assessment procedure.

4. The risk assessment procedure is drawn up in accordance with requirements of national legislation and supervisory authorities in various countries of FMP branches as well as assessments of money laundering and terrorist financing risks carried out by the European Commission and by respective countries on the national level.

POOR PRACTICE

1. The FMP has not established and approved any risk assessment procedure.

2. Even if the FMP performing risk assessment uses other methods for identifying and assessing money laundering and/or terrorist financing risks than those listed in the risk assessment procedure, the risk assessment procedure has not been revised and updated.

3. Risk identification and assessment methods and mathematical models set out in the risk assessment procedure approved by the FMP do not correlate with the risk assessment performed and the risk assessment procedure is formalistic, i.e. it is not followed when carrying out risk assessment.

4. The FMP's risk assessment section Methodology only gives titles (General risks, Geographical risks, Customer profile risks, Payment channel risks, Product risks, Individual whitelists and blacklists) but there is no detailed information on risk identification and assessment methods, which makes it difficult to understand the calculations included in the risk assessment.

4.2. RELEVANCE OF RISK ASSESSMENT

REQUIREMENTS IN THE GUIDELINES

28. The FMP shall ensure that the business-wide ML/TF risk assessment is performed, revised and updated regularly, at least once a year and/or upon any significant change.

38. Prior to starting to provide a new financial service (product) or before starting to provide an existing financial service (product) to a new customer segment, in a new geographical area or through a new delivery channel, the FMP shall assess related ML/TF risks. It shall also assess the ML/TF-related risks associated to business uses of new or developing technologies (both for new and existing services (products)). Adequate measures for managing (mitigating) the aforementioned risks shall be decided based on the results of the assessment of such a service (product).

Paragraph 6 of the Guidelines obliges FMPs to ensure that the internal control system covers continuous and efficient identification, assessment and management of money laundering and/or terrorist financing risks, which means that the assessment of money laundering and/or terrorist financing risks should not be a one-off task. Although FMPs should perform, revise and update risk assessment with the periodicity set in paragraph 28 of the Guidelines, at the same time the FMP must take steps to control and monitor the process of managing money laundering and/or terrorist financing risks to have a possibility to respond swiftly to risk score fluctuations and take respective measures to manage (mitigate) such risk changes. Money laundering and/or terrorist financing risks should be continuously monitored also because risk factors relating to customer risks, product and service risks and/or transaction risks, country-based and/or geographical area risks, risks

associated with products, services, transactions or service delivery channels are not constant and change. For example, having completed the annual risk assessment and identified not only existing but also emerging risks, the FMP may set certain risk indicators to be monitored continuously or during a certain period, and where such risk indicators change substantially or exceed the acceptable risk score set by the FMP (e.g. the number of high-risk customers, non-resident customers from target territories or high-risk countries or legal entity customers incorporated very recently (e.g. less than 6 or 12 months before) goes up significantly, etc.), the FMP takes additional measures to manage (mitigate) risks.

Risk assessment should also be carried out before the FMP starts to provide a new financial service (financial product) or an existing financial service (financial product) to a new customer segment, in a new geographical area or through a new service or product delivery channel. For example, before deciding to provide services to a new customer segment deemed to pose a higher risk, e.g. because of specific activity aspects (e.g. customers linked with virtual assets, gambling, adult services, investment in high-risk products such as virtual assets or forex) or geographical risks, the FMP should rely on the principle of proportionality and carry out a much more comprehensive risk assessment than for lower-risk customers. The FMP should assess money laundering and/or terrorist financing risk exposure of using new or emerging technologies in business (both new and existing services (products)) and adopt adequate and proportionate measures to manage such risks as identified. For instance, having decided to provide services through a particular channel, e.g. to start non face-to-face customer identification or customer identification while using intermediary services, FMPs should assess whether such customer identification would pose additional money laundering and/or terrorist financing risks for the FMP and whether the FMP has risk management controls in place. As for products, in a similar way, before starting to provide a new product, there is a need to identify and assess money laundering and/or terrorist financing risks posed by the delivery of such a new product and, where necessary, to take additional risk management measures. It should be noted that when identifying and evaluating risks associated with specific products, FMPs should have regard to product risks identified and assessed in the Lithuanian National Risk Assessment of Money Laundering and Terrorist Financing (hereinafter – the NRA) and the European Commission's assessment of money laundering and terrorist financing risks[2]. For instance, the NRA states that banks carrying out risk assessments must identify and assess risks posed by trade financing as a product and adapt monitoring measures for payment transactions mitigating money laundering and/or terrorist financing risks posed by the product.

GOOD PRACTICE

1. The FMP's risk assessment procedure stipulates that risk assessment is carried out on an annual basis but 6 months after the conducted risk assessment, having assessed significantly higher numbers of customers and their transactions, the FMP revised and updated it.

2. The FMP carries out risk assessment when getting ready to provide services to a new customer segment associated with higher money laundering and/or terrorist financing risks (virtual currency exchange operators, customers whose activity concerns gambling, adult services and/or investing in high-risk products). Having completed such risk assessments, the FMP puts in place additional customer identification and transaction monitoring measures as well as transaction limits for customers of the respective segment.

---

[2] Lithuanian National Risk Assessment of Money Laundering and Terrorist Financing, 28 May 2020, http://www.fntt.lt/data/public/uploads/2020/05/final-nra_lt_v3.pdf.
2019 report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, https://ec.europa.eu/info/sites/info/files/supranational_risk_assessment_of_the_money_laundering_and_terrorist_financing_risks_affecting_the_union_-_annex.pdf.

POOR PRACTICE

1. Having conducted a risk assessment in 2017, the FMP fails to establish measures to monitor money laundering and/or terrorist financing risks and to monitor and assess risk fluctuations for 3 years although the FMP has expanded its activity during those years, significantly increased the number of customers, expanded the geographical scope of its customer service without updating its risk assessments for 3 years, i.e. without trying to make sure that money laundering and/or terrorist financing risks remain unchanged and risk management measures in place remain sufficient for managing (mitigating) emerging risks.

2. The FMP has performed a group-level risk assessment but has not considered the specific nature of the FMP branch's activity, the region of activity, customer base and services provided, which is why money laundering and/or terrorist financing risks associated with the FMP branch's activity are not identified and assessed in the risk assessment. Because of that the branch has failed to take measures to manage specific money laundering and/or terrorist financing risks arising in relation to the branch's activity.

3. The FMP carries out a risk assessment before the start of its activity, thus identifying and assessing money laundering and/or terrorist financing risks that the FMP may face in the course of its activity, given the business model to be used by the FMP. Later on the FMP changes the business model but takes no account of that when updating its risk assessment and does not rely on any statistical data, which means that the updated risk assessment only identifies and assesses theoretical money laundering and/or terrorist financing risks.

4. Even though the FMP has undergone many significant changes relating to its organisational structure, the definition of its risk appetite, the implementation of new processes and systems and the improvement of technical processes, the FMP's risk assessment is not revised and updated.

4.3. PROPORTIONALITY OF RISK ASSESSMENT TO THE SIZE AND NATURE OF THE FMP'S ACTIVITY

REQUIREMENTS IN THE GUIDELINES

29. The FMP shall ensure that its risk assessment aiming at assessing business-wide ML/TF risks (irrespective of whether the risk assessment is carried out by the FMP or by using third-party services) is proportionate to the nature and size of activities carried out by the FMP and its services and/or products and is performed taking into account the risks inherent to its activities and their factors as well as the risks identified in the National ML/TF Risk Assessment of the Republic of Lithuania and the European Commission's ML/TF risk assessment.

In accordance with the requirement laid down in paragraph 29 of the Guidelines, the FMP must carry out risk assessments in line with the size and nature of its activity. Having regard to the scope and complexity of its services and products, delivery channels, the usability of services and products for money laundering and/or terrorist financing purposes, the nature of the customer portfolio, the geographical scope of activity of the FMP and its customers and other similar criteria, the FMP assesses the complexity and completeness of risk assessment to be carried out so that it is sufficient to identify and assess money laundering and/or terrorist financing risks associated with the said criteria.

When establishing whether the risk assessment is completed in line with the scope and nature of the FMP's activity, there is a need to consider the above mentioned criteria as a whole. This means that the FMP conducting a risk assessment should consider the specific aspects and the scope of the FMP's customers, products and services provided, the activity of the FMP (the FMP's customers) and/or the territory where payments are made as well as the delivery channel. For example, a bank providing many various and complex

products and services (investment services, trade financing, various bank accounts, money remittances, deposits, loans, etc.) and acting through branches in other countries, having many customers or customers whose activity is associated with higher money laundering and/or terrorist financing risks and performing face-to-face customer identification with customers physically present and non-face-to-face customer identification with the help of electronic means enabling direct video streaming/image transmission and/or using third-party information, etc., should have a complex and comprehensive risk assessment carried out taking into account these criteria. The Risk Factors Guidelines stipulate that FMPs that do not offer complex products or services and that have limited or no international exposure may not need an overly complex or sophisticated risk assessment. As already mentioned, FMPs only providing one type of services such as payment initiation services or account information services, or only utility payment services or other regular services to meet household needs, or services of collecting fines and/or other duties for public authorities and social benefit payment services might not need any complex and comprehensive risk assessment. A risk assessment of a currency exchange operator also providing one service (currency exchange in cash) may be simpler and less complex than in the case of the aforementioned bank but such a risk assessment should in any case include money laundering and/or terrorist financing risks characteristic of the currency exchange office's activity, based on these risk factors.

To carry out a risk assessment the FMP may involve third parties experienced in conducting risk assessments. In accordance with paragraph 29 of the Guidelines, irrespective of the fact that the risk assessment is conducted using the services of third parties, it should be proportionate to the size and nature of the FMP's activity. It should be noted that where the FMP involves third parties to perform risk assessment, it is still the FMP that remains responsible for the quality and results of the risk assessment conducted. To make sure that the FMP can use its risk assessment results delivered by third parties in further activity and properly implement risk management (mitigation) measures identified in the course of the risk assessment, the FMP must understand the risk assessment methodology, the impact of specific risk factors in identifying money laundering and/or terrorist financing risks characteristic of the FMP, the likelihood of risks occurring and their impact, the final risk score, etc.

REQUIREMENTS IN THE GUIDELINES
35. The FMP's business-wide ML/TF risk assessment shall be based on data that would allow for the correct identification of the level of ML/TF risks (e.g. the risk assessment shall include various statistics, i.e. the number of the FMP's customers and their distribution by different risk groups; the number of customers using high-risk products; the number (value) of payment transactions in high-risk countries; the number of customers active in high-risk countries).
37. The FMP shall ensure that when carrying out the business-wide ML/TF risk assessment it relies on up-to-date and objective information.

Risk assessment should be based both on quantitative and qualitative data that should be up-to-date, comprehensive, reliable and capable of revealing money laundering and/or terrorist financing risks to which the FMP is exposed in the course of its activity. Data quality is an important element and a crucial factor for a comprehensive and well-grounded FMP risk assessment. Inaccurate, inadequate or obsolete data may give rise to inaccurate or incomplete conclusions while the risk assessment may identify and assess only a part of money laundering and/or terrorist financing risks to which the FMP is exposed in the course of its activity, which may mean that the FMP will not take necessary and proportionate risk management (mitigation) measures.

REQUIREMENTS IN THE GUIDELINES
30. The FMP's business-wide ML/TF risk assessment shall be performed considering the following:
30.1. customer risk;
30.2. country-specific or geographical risks;
30.3. service/product or operational risks;
30.4. risks relating to delivery channels.
31. Having regard to the nature and size of its activities, the FMP may also identify other risk categories than those listed in paragraph 30 of the Guidelines.

As set out in the Guidelines, a proper and comprehensive risk assessment first of all warrants a deep and thorough understanding of money laundering and/or terrorist financing risks that the FMP may face in the course of its activity. When carrying out a risk assessment, the FMP should identify and categorise risks by types as provided for in paragraph 30 of the Guidelines and identify risk factors affecting money laundering and/or terrorist financing risks.

Even though legislation does not regulate any methodology for identifying and assessing money laundering and/or terrorist financing risks, the FMP performing a risk assessment should choose such risk identification and assessment techniques and methods that would ensure that in the course of its risk assessment the FMP identifies risks arising in its activity and properly assesses such risks.

In line with good practices[3], the FMP performing a risk assessment firstly identifies and assesses inherent money laundering and/or terrorist financing risks, evaluates the effectiveness of risk management measures covering money laundering and/or terrorist financing risks put in place by the FMP and only then assesses residual risks. The analysis of FMP risk assessments carried out by the Bank of Lithuania has shown that in practice FMPs most often use such a methodology for identifying and assessing money laundering and/or terrorist financing risks that covers inherent risks, risk control effectiveness and residual risks. It should be noted that the FMP may also identify and assess the level of money laundering and/or terrorist financing risks based on threat and vulnerability or choose other ways and methods for identifying and assessing money laundering and/or terrorist financing risks[4].

To make sure that inherent money laundering and/or terrorist financing risks are identified as comprehensively as possible, a risk assessment should cover all products and services provided by the FMP (e.g. including services provided in the European Union when exercising the freedom to provide services, services provided through intermediaries, etc.). Where the FMP has branches in other countries, when carrying out a risk assessment it should consider the services of such branches or their risk assessments.

It should be noted that risks associated with products and services and delivery channels pertaining to customers, countries and/or regions may be identified by analysing data from various viewpoints. It is not only the number of customers that might be evaluated during the risk assessment, but also customer turnover with a view to disclosing risks fully and avoiding cases where the turnover of a handful of higher-risk customers accounts for a major part of the total turnover of the FMP's customers but in terms of their number such customers are few and the risk they pose is therefore not identified accurately. For example, when identifying and assessing inherent customer risks one may consider the number and turnover of politically

---

[3] Wolfsberg Group: Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery and Corruption, https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/faqs/17.%20Wolfsberg-Risk-Assessment-FAQs-2015.pdf.

[4] Recommendations of the International Organization for Standardization (ISO 31000:2018(en) *Risk management – Guidelines*), https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en.

exposed persons (hereinafter – PEPs), the number and turnover of customers engaging in activities associated with higher risks, etc.; when identifying and assessing inherent country-based and/or geographical area risks one may consider the number and turnover of customers whose place of registration or residence is in high-risk third countries, payments received from high-risk third countries, etc.; when identifying and assessing inherent risks associated with services and products provided and transactions performed one may consider all products and services provided by the FMP (e.g. cash services, trade financing products, etc.); when identifying and assessing inherent risks associated with products, services, transactions or delivery channels one may consider the number and turnover of customers with non-face-to-face customer identification, the number and turnover of customers identified while using services of intermediaries, etc.

To establish whether it is necessary to put in place additional management measures for money laundering and/or terrorist financing risks, in the course of its risk assessment the FMP should assess the effectiveness and adequacy of its existing risk management measures. Having assessed existing risk management measures, the FMP assesses residual money laundering and/or terrorist financing risks by risk types listed in paragraph 30 of the Guidelines. It should be noted that residual risks should be assessed so that they are real and not diminished, i.e. the FMP should not show money laundering and/or terrorist financing risks as lower than they are.

GOOD PRACTICE

1. The risk assessment separately identifies and assesses money laundering and terrorist financing risks and also identifies and assesses risks associated with international financial sanctions and proliferation financing.

2. When assessing customer risks the FMP considers any specific aspects of activity of natural and legal persons, customer activity segments and risk groups taking into account customers' legal form, maturity, transactions (their types, the share of cash, the proportionate shares of payments made in the Republic of Lithuania, in the European Union and internationally, the share of payments to target territories or high-risk countries, etc.), geographical risks from various perspectives (e.g. for natural persons by nationality, by place of residence, by place of tax residence; for legal entities by place of establishment, by place of business, by place of main partners, by nationality or place of residence of beneficial owners, etc.).

3. The risk assessment takes account of other important aspects such as the stability of the customer base, system integration, human resources, third-party services, projected growth of the number of customers or transactions, the number of complaints relating to customer services, the number of law-enforcement inquiries, etc.

4. The risk assessment not only identifies risks but also thoroughly evaluates preventive controls for money laundering and/or terrorist financing risks put in place by the FMP. There is normally a questionnaire thoroughly assessing various processes and their effectiveness (customer identification, beneficial owner identification, customer risk identification and assessment (whether all factors are taken into account), updates of customer and beneficial owner details, enhanced customer due diligence and enhanced monitoring of business relationships with high-risk customers, screening of international sanctions and PEPs, monitoring of operations and transactions (systems used, investigations conducted and relevant documentation, escalation of internal investigation information to senior management, notifications to the FCIS, etc.).

POOR PRACTICE

1. The risk assessment does not cover relevant for FMP risks identified in the Lithuanian National Risk Assessment of Money Laundering and Terrorist Financingand the European Commission's assessment of money laundering and terrorist financing risks (e.g. does not assess risks associated with cash transactions, the delivery of trade financing products, etc.).

2. The FMP does not have sufficient data on all products and services provided by the FMP, which renders the product risk assessment incomplete. Even though the risk assessment states that "the inability to provide such information reduces the effectiveness of inherent product risk assessment", the FMP has failed to put in place any measures to ensure that in the future that data on products and services are comprehensive.

3. Although the FMP's risk assessment states that the customer risk assessment process needs to be improved and that there are certain shortcomings relating to customer risk assessment, monitoring of transactions, delivery of products and identification of suspicious transactions but the inherent risk is deemed to be low, the effectiveness of all controls is deemed adequate and the residual risk is assessed as low.

4. The risk assessment does not take account of internal control testing results for assessing the effectiveness of such risk management measures. For example, the compliance risk assessment states that the customer transaction monitoring process put in place by the FMP has significant deficiencies but the risk assessment deems the controls to be adequate.

5. The risk assessment does not provide a comprehensive assessment of risk factors associated with geographical risks (e.g. to which specific jurisdictions the FMP's customers (their beneficial owners) belong, where they carry out their activities, with which jurisdictions or territories the transactions conducted are associated, etc.).

6. The assessment of inherent risks is based only on a small share of data at the FMP's disposal (e.g. customer risks are assessed taking into account only the customer's place of residence and risk group (high or low); product risks are assessed taking into account the customer's place of residence and any changes concerning customers who are PEPs). The risk assessment does not specify what data have been analysed when identifying geographical risks and risks associated with product and service delivery channels.

7. There is no indication of the base used in the risk assessment to establish when risks are deemed low, medium or high and in what cases controls are deemed adequate.

8. The residual risk score is calculated as low even though inherent risks are high and controls are deemed inadequate.

9. The FMP has failed to explain to the supervisory authority how the risk is calculated in the risk assessment and what weighing factors are used to assess the risk because the FMP has relied on risk assessment results automatically calculated by the system.

4.4. RISK ASSESSMENT DOCUMENTATION AND PRESENTATION OF ITS RESULTS TO THE FMP'S MANAGEMENT

REQUIREMENTS IN THE GUIDELINES
32. All business-wide ML/TF risk assessments performed by the FMP and subsequent amendments and/or updates relating to such risk assessments shall be documented. The FMP's management body and audit committee and, where it is not required to establish one, – the supervisory board, if established, shall be informed about the results of the FMP's business-wide ML/TF risk assessment.

The Guidelines contain an obligation for the FMP to document and store information relating to the performance of risk assessment and its revision and updating. The storage of such information ensures that the FMP will monitor any changes in the level of money laundering and/or terrorist financing risks and the effectiveness of respective risk management measures. The analysis of FMP risk assessments conducted by the Bank of Lithuania has shown that some FMPs store the entire data and information package relating to risk assessments including the risk assessment procedure, risk identification and assessment methodology,

the package of data and information used, information provided to persons coordinating risk assessments of various FMP units, risk calculation documents, the risk assessment report, etc., which is considered good practice. It should be noted that storing risk assessment information that is both comprehensive and abundant enough to make it possible to draw similar conclusions on the identification and assessment of money laundering and/or terrorist financing risks to which the FMP is exposed in the course of its activity ensures that the conclusions of the FMP's risk assessments are comparable with one another, thus monitoring any temporal developments in money laundering and/or terrorist financing risks.

The FMP's senior management should be notified about risk assessment results and kept abreast of money laundering and/or terrorist financing risks, risk scores and any related changes for the purpose of making decisions, allocating resources and establishing strategic directions for the FMP. It is important that both the management and the staff understand that the main objective of risk assessment is to identify money laundering and/or terrorist financing risks with a view to establishing proper and adequate risk management measures. It should be noted that the FMP's senior management's attention to risk assessment and the implementation of the risk management (mitigation) action plan enables the management to make decisions based on information at their disposal on money laundering and/or terrorist financing risks to which the FMP is exposed in the course of its activity and on the adequacy and effectiveness of respective risk management measures; the tone from the top also helps the FMP staff to get a better understanding of the importance of risk assessment and lays the groundwork for a risk assessment that is not formalistic (bureaucratic) and encourages the FMP to develop a risk management culture.

GOOD PRACTICE

1. The FMP board receives the risk assessment report and the action plan for managing (mitigating) money laundering and/or terrorist financing risks. The FMP board approves the risk management (mitigation) action plan at the same time obliging the responsible FMP division to inform the board about its implementation on a quarterly basis.

POOR PRACTICE

1. Risk assessment results are submitted to the FMP's head of administration but not to the FMP board.

2. The FMP prepares a brief report on risk assessment results describing the services provided by the FMP and stating that the overall level of the FMP's money laundering and/or terrorist financing risks is medium and the FMP manages all money laundering and/or terrorist financing risks, which is why no additional risk management measures are needed. The FMP has no risk assessment procedure and does not store any methodology for identifying and assessing money laundering and/or terrorist financing risks, a data analysis package or other information making it possible to understand how risks have been identified and assessed, how the effectiveness of the FMP's controls has been assessed and how the medium risk score has been calculated.

4.5. RISK MANAGEMENT (MITIGATION) ACTION PLAN

REQUIREMENTS IN THE GUIDELINES
34. Having performed the business-wide ML/TF risk assessment and established that the applied risk management (mitigation) measures are not sufficient, the FMP shall prepare a risk management (mitigation) action plan that shall be approved by the FMP's management body or a person authorised thereby.

As already mentioned, risk assessment must not be an end in itself and must be useful for the FMP, which means that risk assessment must be used in the FMP's future activities. The Guidelines stipulate that where a risk assessment shows that the existing measures put in place by the FMP to manage money laundering and/or terrorist financing risks identified by the FMP are not sufficient, there is a need to prepare a risk management (mitigation) action plan. It should be noted that a risk management (mitigation) action plan may be omitted and no risk management (mitigation) measures may be taken only where the FMP has adequate and proportionate measures to manage money laundering and/or terrorist financing risks identified in the risk assessment. To ensure that the measures listed in the risk management (mitigation) action plan are adequate for managing money laundering and/or terrorist financing risks identified in the course of risk assessment, the FMP should ensure that the implementation of the measures listed in the risk management (mitigation) action plan is the responsibility of the FMP staff (business units) and that the implementation of such measures is being monitored and evaluated.

GOOD PRACTICE
1. The FMP has performed a risk assessment and prepared a risk management (mitigation) action plan approved by the FMP's management body and setting specific deadlines for implementing additional measures to manage money laundering and/or terrorist financing risks.
2. The risk management (mitigation) action plan contains clear provisions on identifying the areas to be improved, appointing responsible persons and setting implementation deadlines; there are regular progress checks of the plan implementation, the effectiveness of actions performed is evaluated and FMP management is regularly informed about the plan implementation progress.
3. The risk management (mitigation) action plan includes such measures as additional training for the FMP staff on the topic of higher-risk jurisdictions (including money laundering typologies in such jurisdictions) and the implementation of international financial sanctions; additional monitoring measures for customer risk assessment and categorisation; changes in the transaction monitoring system relating to the specific aspects of the trade financing product; a more frequent process of updating details on customers subject to complaints or law-enforcement inquiries; implementation of new transaction monitoring rules under enhanced continuous monitoring of business relationships; analysis of the portfolio of the high-risk group of customers every 6 months; technical system modifications ensuring the dual control mechanism; recruitment of additional staff for transaction monitoring, etc.

POOR PRACTICE

1. The FMP has no risk management (mitigation) action plan or the existing plan has no effect on further management, monitoring and control processes for money laundering and/or terrorist financing risks.

2. The measures listed in the risk management (mitigation) action plan are not in line with the risk assessment and the FMP takes no measures to manage (mitigate) the money laundering and/or terrorist financing risks identified.

3. Even though the risk assessment has shown that the monitoring measures for customer business relationships and transactions put in place by the FMP are inadequate for monitoring higher-risk customer transactions, the measures established in the risk management (mitigation) action plan only target changes in the FMP's internal procedures without actually implementing any additional measures relating to the monitoring of transactions.

4. The risk management (mitigation) action plan contains the only measure, which is third-party audit, and it is not clear how this measure will help the FMP to manage the money laundering and/or terrorist financing risks identified in the course of risk assessment.

5. The risk assessment has established that the residual money laundering risk posed by a trade financing product is high while the terrorist financing risk is medium stressing that the complexity of the product requires specialised knowledge to assess product-related payments and documents but the risk management (mitigation) action plan does not provide for any measures to manage such product risks.

6. There is no clear process as to who is responsible for the implementation of the risk management (mitigation) action plan and by what deadlines. The risk management (mitigation) action plan presented to FMP management is not implemented due to the lack of attention on behalf of the FMP management to the plan and/or its implementation control.