ESTONIAN ENTREPRENEURSHIP UNIVERSITY OF APPLIED SCIENCES
Enterprise Strategic Management

Makhmud Makhmudov

MONEY LAUNDERING AND TERRORIST FINANCING RISK MANAGEMENT IN THE PROCESS OF CLIENT'S VERIFICATION OF LEI REGISTRATION AGENT LEIPAPA OÜ

Master's thesis

Supervisor: Suzanna Kalinina, MD
Co-supervisor: Nikolay Kalinin, MD

Tallinn 2022

Present master's work has been done by me independently.
All works of other authors, fundamental points of view
and other data from literary and other sources
used in this master's work are given with links.

The author: Makhmud Makhmudov …….

(signature and date)

RESUME

The title of the current research work is "Money laundering and terrorist financing risk management in the process of Client's verification of LEI Registration Agent LEIpapa OÜ".

The relevance of the thesis is confirmed by the need to identify and assess risks related to money laundering (ML) and terrorist financing (TF) within the framework of Registration Agent due to the high level of causes of ML/TF and the significant addition of relevant persons to the sanctions lists due to current geopolitical situation; requests from representatives of Global Legal Entity Identifier Foundation (GLEIF) and the managing Local Operating Unit (LOU) for the implementation of the system allowing to use technical means within the workflow of Client's verification and assess the ML/TF risks arising during the verification process; the need to improve Company's strategy to reduce costs and comply with the requirements of regulatory authorities; the desire of the Company's management to obtain the status of Validation Agent in partnership with a financial institution.

The study aims to develop an ML/TF Risk Management Framework for the process of Legal Entity verification of LEI Registration Agent LEIpapa OÜ.

The object of the study is the workflow of the Client's verification at LEIpapa OÜ. The subject of the study is the ML/TF risks associated with the object under study.

The provisions and conclusions on solving the problems of risk management in the field of ML/TF contained in the guidelines, legislative acts, and regulations from authorities were used for the theoretical and methodological basis of the study. The nature of the objectives set and a systematic approach to their solution determined the use of the following research methods in the study: method of operational diagnostics (analysis of the current workflow of the Clients' identification and verification; analysis of ML/TF risks the Company manages, etc.), synthesis, Delphi method, generalization, and other general scientific methods. The legislative basis for conducting an ML/TF risk assessment is based on the International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation from the Financial Action Task Force (FATF); Requirements of Estonian Money Laundering and Terrorist Financing Prevention Act (MLTFPA); Guidelines of Basel Committee on Banking Supervision; the advisory guidelines established by resolution no. 1.1-7/172 of the Management Board of Estonian Financial Supervisory Authority (FSA) of

26 November 2018; EU Markets in Financial Instruments Directive II (MiFID II) and EU Markets in Financial Instruments Regulation (MiFIR) legislative frameworks.

The Company's internal and public data, Internet sources, normative-legal acts, and the author's previous research results were used as an information base for the research.

The study has both theoretical and practical significance since the author holds a position of a Board Member in the Company and leads the process of implementing the feature of automated verification of Legal Entities with the use of technical means provided by third parties, along with the developing of ML/TF Risk Management Framework. Despite the presence of numerous publications on the essence and specifics of the implementation of international and European procedures related to anti-money laundering and counter-terrorist financing (AML/CFT) in the activities of obliged entities, a little attention in dissertation research is given to the issue of ML/TF Risk Management Framework implementation, as well as studying the features of the functioning of Estonian-based LEI Registration Agents and Validation Agents in the field of AML/CFT.

The work consists of a list of definitions, an introduction, three chapters, a conclusion, and a list of references and applications. The total volume of work is 169 pages which contain 8 tables, 7 figures, 1 formula, and 13 appendices.

RESÜMEE

Käesoleva uurimistöö teemaks on "Rahapesu ja terrorismi rahastamise riskide juhtimine LEI registreerimisagendina LEIpapa OÜ kliendi tuvastamise protsessis".

Töö aktuaalsust kinnitavad: vajadus tuvastada ja hinnata rahapesu ja terrorismi rahastamisega seotutud riske LEI registreerimisagendi raames, kõrge rahapesu tase, sanktsioonid ja praegune geopoliitiline olukord kui ka tuvastamise süsteemi rakendamise taotlus ülemaailmse juriidiliste identifikaatori sihtasutusest GLEIF ja haldava kohaliku operatiivüksusest LOU esindajate poolt; süsteemi, mis võimaldaks kasutada kliendi tuvastamise protsessi raames tehnilisi vahendeid ja hinnata tuvastamise protsessi käigus tekkivaid rahapesu ja terrorismi rahastamisega seotud riske ning ka vajadus täiustada ettevõtte strateegiat kulude vähendamiseks ja reguleerivate asutuste nõuete jälgimiseks, kui ka ettevõtte juhtkonna soov saada koostöös finantsasutustega valideerimisagendi staatust.

Käesoleva töö eesmärk on töötada välja rahapesu ja terrorismi rahastamise tõkestamiseks riskijuhtimise raamistikku LEI registreerimisagendi LEIpapa OÜ-le juriidilise isiku tuvastamise protsessis.

Uuringu objektiks on kliendi tuvastamisel tekkitav töövoog LEIpapa OÜ-s. Teema uurimissuunad on uuritava objektiga seotud riskid rahapesu tõkestamise valdkonnas.

Teoreetiliseks ja metoodiliseks aluseks kasutas autor erinevad juhendid, õigusaktid ja ametiasutuste määrused antud valdkonnas. Antud ülesannete iseloom ja süstemaatiline lähenemine nende lahendamiseks määras kasutada järgmisi uurimismeetodeid: operatsiooni diagnostika (klientide tuvastamise ja jooksva töövoogu kontrolli analüüs; ettevõtte juhitavate rahapesu ja terrorismi rahastamisega seotud riskide analüüs jne), süntees, Delphi meetod, üldistus ja muud uurimismeetodid. Rahapesu ja terrorismi rahastamise riskihinnangu läbiviimise seadusandlik alus põhineb rahapesu ja terrorismi rahastamise vastase võitluse rahvusvahelistel standarditel, mille on koostanud Financial Action Task Force (FATF); Eesti Vabariigi rahapesu ja terrorismi rahastamise tõkestamise seaduse (MLTFPA) nõuetel; Baseli pangajärelevalve komitee suunisel; otsusega nr 1.1-7/172 Finantsinspektsiooni (FSA) juhatuse 26.11.2018 määrusel. EL finantsinstrumentide turgude direktiivil II (MiFID II) ja EL finantsinstrumentide turgude määrusel (MiFIR) õigusraamistikud.

Uurimis töö infobaasi allikana kasutas autor ettevõtte sisemised ja avalikud andmeid, Interneti allikaid, normatiivakte ja autori varasemate uuringute tulemused.

See uuring on teoreetilise kui ka praktilise tähtsusega, kuna autor on ettevõttes juhatuse liikme ametikohal ja juhib juriidiliste isikute automaatse tuvastamise funktsiooni seadmist kolmandate isikute pakutavate tehniliste vahendite abil koos rahapesu ja terrorismi rahastamise tõkestamiseks riskijuhtimise raamistiku väljatöötamisega. Hoolimata rakendamise olemust ja eripära käsitlevate arvukate publikatsioonide (rahvusvahelised ja Euroopa), mis on seotud rahapesu ja terrorismi rahastamise tõkestamisega olemasolu, vähe tähelepanu pööratakse kohustatud isikute tegevusele, mida on seotud käesolevas uurimistöös käsitletava teemaga - riskijuhtimise raamistiku rakendamine kui ka Eestis asuvate LEI registreerimis- ja valideerimisagentide funktsioonide uurimine rahapesu ja terrorismi rahastamise tõkestamise valdkonnas.

Töö koosneb mõistete loetelust, sissejuhatusest, kolmest peatükist, järeldusest ning kasutatud kirjanduse loetelust ja lisadest. Töö kogumaht on 169 lehekülge, mis sisaldab 8 tabelit, 7 joonist, 1 valemit ja 13 lisa.

TABLE OF CONTENTS

DEFINITIONS

In this thesis and/or any of its accompanying supplements the following words and expressions shall have the following meanings attributed to them below:

Anti-Money Laundering or **AML** – Anti-money laundering.

AMLD – Directive (EU) 2018/843 (2018), also known as the "Fifth Anti-Money Laundering Directive", of the European Parliament and the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU.

Board Member or collectively referred to as **Board Members**, or the **Board** – A person(-s) appointed to hold the office of a Board Member(-s) of the company and who is (are) assigned to perform a management or supervisory function.

Company – LEIpapa OÜ, a company with the registry code 16283000 established under the laws of the Republic of Estonia. LEIpapa OÜ is an official Registration Agent and acts according to the License Agreement concluded with GLEIF.

CDD or **Customer due diligence** – The process of establishing customer identities.

CFT – Counter-terrorist financing.

EBA – The European Banking Authority, is an independent EU Authority that works to ensure effective and consistent prudential regulation and supervision across the European banking sector. Its overall objectives are to maintain financial stability in the EU and to safeguard the integrity, efficiency, and orderly functioning of the banking sector (European Banking Authority (EBA), 2016).

Financial Action Task Force or **FATF** – An independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing, and the financing proliferation of weapons of mass destruction (FATF, 2021).

Finantsinspektsioon or **FSA** or **Estonian Financial Supervision and Resolution Authority** – The legal entity of public law, which is established, and operates under the laws

of the Republic of Estonia and conducts state financial supervision to enhance the stability, reliability, transparency, and efficiency of the financial sector, to reduce systemic risks and to promote the prevention of the abuse of the financial sector for criminal purposes, to protect the interests of customers and investors by safeguarding their financial resources, and thereby supporting the stability of the monetary system of the Republic of Estonia (Financial Supervision Authority Act, 2022, subsection 3 (1)).

FIU or **Estonian Financial Intelligence Unit** or ***Rahapesu Andmebüroo*** – The Unit for Combating Money Laundering was established as the national center for receiving, requesting, analyzing, and disseminating disclosures of suspicious transactions reports and other relevant information concerning suspected money laundering and terrorist financing (Ministry of Finance, 2022).

FSB or **Financial Stability Board** – is an international body that monitors and makes recommendations about the global financial system and promotes international financial stability. Working through its members, the FSB seeks to strengthen financial systems and increase the stability of international financial markets. The policies developed in the pursuit of this agenda are implemented by jurisdictions and national authorities (FSB, 2020).

Global Legal Entity Identifier Foundation or **GLEIF** – A supra-national not-for-profit organization headquartered in Basel, Switzerland, established by the Financial Stability Board in June 2014 and tasked to support the implementation and use of the LEI. The foundation is backed and overseen by the Regulatory Oversight Committee, representing public authorities from around the globe that have come together to jointly drive forward transparency within the global financial markets (GLEIF, 2021a).

Global LEI Index – The Global Legal Entity Identifier Index, contains historical and current LEI records including related Reference Data in one authoritative, central repository. The Reference Data provides the information on a Legal Entity identifiable with an LEI. The Global LEI Index is the only global online source that provides open, standardized, and high-quality Legal Entity Reference Data (GLEIF, 2021d).

Global LEI System – The system, that through the issuance of LEIs provides unique identification of Legal Entities participating in financial transactions across the globe (GLEIF, 2021b).

Know Your Client or **KYC** – A set of standards used within the investment and financial services industry to verify customers, their risk profiles, and their financial profiles (Chen, 2021).

Legal Entity or **Client** – An entity, other than a natural (physical) person, created by law and recognized as a legal entity with separate legal personality, duties, and rights.

Legal Entity Identifier or **LEI** or **LEI Identifier** or **LEI Code** – a 20-character, alpha-numeric code based on the ISO 17442 standard developed by the International Organization for Standardization (ISO) (Ubisecure OY, 2019, 3).

Legal Entity Reference Data or **LE-RD** – Presented within a Common Data Format (CDF) structure Legal Entity Reference Data (LE-RD) covers items such as Legal Entity Form, Legal Entity Status, Legal Name, and Legal Entity Address (Ubisecure OY, 2019, 12).

LEI Record – An XML data record in LEI-CDF format describing one legal entity (Ubisecure OY, 2019, 12).

LEI ROC – LEI Regulatory Oversight Committee is a group of more than 65 financial markets regulators and other public authorities and 19 observers from more than 50 countries established in November 2012 to coordinate and oversee a worldwide framework of legal entity identification, the Global LEI System. It promotes the broad public interest by improving the quality of data used in financial data reporting, improving the ability to monitor financial risk, and lowering regulatory reporting costs through the harmonization of these standards across jurisdictions (ROC, 2022).

LOU or **Local Operational Unit** – A LEI issuing organization, approved by GLEIF, that supplies registration, renewal, and other services, and act as the primary interface for Legal Entities wishing to obtain an LEI (GLEIF, 2022a).

Managing LOU or **LEI Issuer** – The LOU which manages and maintains the data of an LEI (GLEIF, 2022a).

MiFID II – Markets in Financial Instruments Directive II (EU).

MIFIR – Markets in Financial Instruments Regulation (EU).

MLTFPA (*RahaPTS*) – The Money Laundering and Terrorist Financing Prevention Act of the Republic of Estonia, RT I, 17.11.2017, 2, and any law substituting or amending the same (MLTFPA, 2022).

ML/TF – Money laundering and terrorist financing.

Registration Agent or **LEI Registration Agent** – A third-party service provider that assists the Managing LOU with the performance of its duties in the Global LEI System, acting based on the license agreement concluded with GLEIF and registration agent agreement concluded with the Managing LOU (GLEIF, 2020).

Risk Framework or **Risk Management Framework** – The totality of risk policies (a set of formal instructions, typically documented and approved by internal governing bodies, that define insufficient operational detail an organization's perception and attitude towards the range of risks it faces and desires to manage), internal risk management processes (a well-defined activity within an organization that aims to identify, measure, or mitigate risks) and risk tools used by an organization to manage the variety of risks it is facing (Open Risk Manual, 2021).

Validation Agent – an organization that obtains and maintains LEIs for its clients in cooperation with accredited LEI Issuers by leveraging their business-as-usual client identification procedures in Know Your Customer (KYC) and client onboarding processes (GLEIF, 2022b).

INTRODUCTION

The issue of money laundering (ML) and the financing of terrorism (TF), has recently acquired a relevance, becoming truly international. This phenomenon not only harms the economic security and financial stability of a particular country but also makes it difficult to investigate and solve crimes and undermines the reputation of entities having the obligation to implement due diligence measures for the prevention of ML/TF and inform relevant authorities about suspicions or cases related to ML/TF (the so-called "obliged entities" under MLTFPA (2022, sec. 2, p.2)), number of which has increased. For example, banks, entrepreneurs providing financial services, organizers of games of chance, intermediaries in transactions with real estate, pawnbrokers, auditors, and entrepreneurs who provide accounting or consulting services, as well as service providers are all defined as obliged entities. As practice shows, the risk of involvement of obliged entities in the processes of legalization of criminal proceeds exists both at the international and national levels. For Estonia, it is especially dangerous because it can lead to the loss of the business reputation of the obliged entity and, accordingly, will become an obstacle to the expansion of activities in the global financial markets. Non-compliance with laws and procedures aimed at anti-money laundering (AML) and counter-terrorist financing (CFT), the ineffectiveness of the internal control of the obliged entity, may lead to the emergence of this risk. An overview of the extent of this threat can be found in the reports of the Financial Intelligent Unit (FIU) discussed in section 1.3. of this thesis and in National Risk Assessments reports published every two years by the Ministry of Finance of Estonia and available publicly.

To identify legal entities involved in financial transactions and other valued transactions between corporations or legal entities, a Legal Entity Identifier (LEI) global standard was designed and defined by the ISO 17442, in the spirit of public and private partnership to improve transparency in the marketplace for entities and regulators alike and to collate financial transaction information into a freely accessible Global LEI System (ManagedLEI, 2021). In June 2012 at Los Cabos Summit (FSB, 2012b), the G20 Leaders endorsed the Financial Stability Board (FSB) report "A Global Legal Entity Identifier for Financial Markets" (FSB, 2012a) and encouraged "global adoption of the LEI to support authorities and market participants in identifying and managing financial risks" (FSB, 2019, 1). Regulated by the Regulatory Oversight Committee (ROC) through the Global Legal Entity

Identifier Foundation (GLEIF), LEI is a 20-character identifier that represents a distinct legal entity engaged in financial transactions and the purpose of LEI is to be the single organization identity behind every business (LEIregister, 2021). To streamline the process of issuing LEIs, GLEIF has introduced the concept of "Registration Agents" (GLEIF, 2018b). The Registration Agent is an obliged entity, that acts according to a license agreement with GLEIF, and facilitates the interaction of Clients (Legal Entities) with the network of organizations called Local Operating Units (LOUs) that issue LEIs and provide related services. Legal Entities are required to notify the LOU they work with (Managing LOU) of any changes to their Reference Data. The annual mandatory renewal process allows Clients and LOUs to re-verify and confirm the correctness of the submitted Reference Data. This ensures the high quality of the data in the Global LEI database and thus the credibility of the Global LEI System.

According to data obtained via email communication with a representative of Managing LOU on March 14th, 2022 (the email is in the author's possession), the concept of Registration Agents is relatively new, and currently, LEI Registration Agents don't use a fully functional ML/TF Risk Management Framework for Client identification and verification, since LOUs ask them to collect the Client data and corporate documents, performing pre-search in the corporate register, and forward the data obtained through the internal system to LOU for further Client identification and verification. The author was also informed that LOUs are trying to understand if even a Validation Agents will be able to collect trustworthy data. That's why LOUs and the GLEIF will dive into Know Your Customer (KYC) and Client Onboarding Procedures during parts of the Validation Agent's Onboarding Workflow (Appendix 1). Since Registration Agents don't perform the identification and validation with their resources, they don't use technical (automated) means for Client verification when there is no information about the Client and its beneficial owners in the corporate register found during pre-search (such cases may happen if the Client is a fund, will pension, or trust). Thus, Registration Agents spend unnecessary financial and human resources on manual work and allow the risk of fraud and chargebacks to occur when the wrong data is obtained. Besides, in the case when significant and constant work with a large Client data flow is expected and technical means are not used, the internal control of the Registration Agent may be ineffective due to human factors (weaknesses), which is a gross violation of the law and may result in a significant monetary penalty (as per MLTFPA) or revocation of the license of the Registration Agent.

The number of LEI challenges received, and the monthly quality issues reported for the top three LOUs (RapidLEI, GMEI Utility, and Bloomberg LEI) are represented in Figure 1.

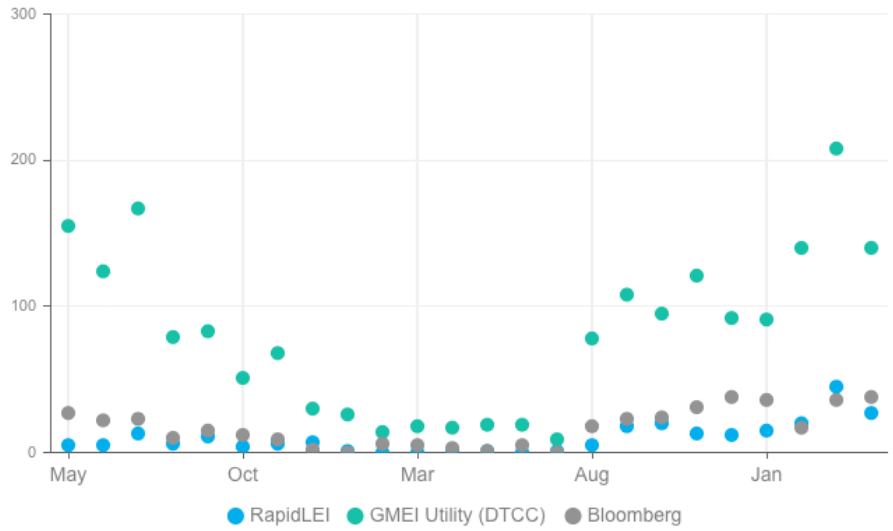


Figure 1. LEI Data Quality as reported by the GLEIF. Challenges made on data accuracy.

Source: https://rapidlei.com/stats/

The issues in Legal Entity Reference Data impact the ability to achieve the new LEI Conformity Flag, which is an important addition to the LEI record, as it is active when the LEI is in overall conformity, giving enhanced trust and reliability for the LEI Reference Data it represents (Waite, 2020).

Automating the process of interaction between Clients (Legal Entities) and Registration Agents can reduce the execution time and optimize the costs of the Registration Agent's service, excluding the possibility of chargeback cases, and improving the reliability and quality of data in the Global LEI System. However, even with the help of an automated system for Client verification, according to requirements from regulators and supervising entities, the Registration Agent must use a risk-based approach and be able to identify, assess and understand the ML/TF risks to which it is exposed to and take the necessary AML/CFT control measures to mitigate them. Such requirements are also constantly changing under the influence of the following factors:

- changes in the regulatory system (since 2015, the MLTFPA has been completely changed four times, the last revision was made on March 15, 2022);
- tightening of sanctions nowadays according to the geopolitical situation;
- number of revoked licenses of the obliged entities in Estonia;

- the use of offshore companies to hide the origin of funds, corruption, and bribery;
- scandals related to the participation of various financial organizations in different schemes related to ML/TF;
- the problem associated with the implementation of a risk-based approach has not been resolved and requires more attention in research;
- strengthening the country's position in the international arena.

Having a fully functional ML/TF Risk Management Framework, Registration Agent can apply for updating its status to the status of Validation Agent in partnership with a financial institution, and issue LEIs for organizations, funds, and trusts (including the upcoming Verified LEI (vLEI)) using implemented KYC, AML and Compliance-as-a-Service workflows to obtain LEIs for Clients when verifying a Client's identity. Validation Agents approved by GLEIF are enabled to purchase and manage LEIs at reduced costs, increasing the profitability of their business compared to Registration Agents; and that's the main strategic aim of the Board of the Company to obtain the status of Validation Agent.

The relevance of the thesis is confirmed by:

- the need to identify risks within the framework of Registration Agent due to poor understanding of ML/TF risks by such businesses, the high level of cases related to ML/TF, and the significant addition of relevant persons to the sanctions lists;
- requests from representatives of GLEIF and LOU for the implementation of the system allowing the use of technical means within the workflow of the Client's verification, and performance of the assessment of the ML/TF risks arising during the verification process;
- the need to improve the Company's strategy to reduce costs and comply with the requirements of regulatory authorities;
- the Company's management intention for obtain the status of Validation Agent in partnership with a financial institution.

This study has both theoretical and practical significance since despite the presence of numerous publications on the essence and specifics of the implementation of international and European AML/CFT procedures in the activities of obliged entities, a little attention in dissertation research is given to the issue of ML/TF Risk Management Framework implementation, as well as studying the features of the functioning of Estonia based LEI Registration Agents and LEI Validation Agents in the field of AML/CFT.

The object of the study is the workflow of the Client's verification at LEIpapa OÜ. This Company was chosen for the study since the author holds a position of a Board Member of the Company and leads the process of implementing the feature of automated verification of the Clients with the use of technical means provided by third parties, along with the

preparation of Risk Management Framework related to ML/TF. The subject of the study is the ML/TF risks associated with the object under study.

The study aims to develop an ML/TF Risk Management Framework for the process of Legal Entity verification of LEI Registration Agent LEIpapa OÜ. The author set the following research objectives to achieve the aim of the study:

- define money laundering and terrorist financing, analyze legislative acts, guidelines, and recommendations related to ML and TF from FATF, Estonian FSA, and FIU, define competent authorities engaged in the prevention of ML and TF in Estonia; identify, assess, and categorize risks related to ML/TF that the Registration Agent is facing when performing verification of Legal Entities; summarize scientific and regulatory understandings of the ML risk management for the Registration Agent;
- provide the characteristics of LEIpapa OÜ, investigate the risk factors of the Registration Agent in the area of AML/CFT and identify the main problems in the current risk assessment system; determine legislative possibilities for verifying Clients using technical means provided by a third party; analyze the capabilities of the third-party verification system and its applicability for using within the workflow of Registration Agent;
- based on the results obtained, develop the ML/TF Risk Management Framework of LEIpapa OÜ and assess the applicability of its usage within the structure of the Validation Agent.

The provisions and conclusions on solving the problems of risk management in the field of ML/TF contained in the guidelines, legislative acts, and regulations from authorities were used for the theoretical and methodological basis of the study. The nature of the objectives set and a systematic approach to their solution determined the use of the following research methods in the study: method of operational diagnostics (analysis of the current risk assessment used in the Company; analysis of ML/TF risks the Company faces, etc.), synthesis, Delphi method, generalization, and other general scientific methods. The legislative basis for conducting an ML/TF risk assessment is based on:

- International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation from FATF;
- Requirements of MLTFPA;
- Guidelines of Basel Committee on Banking Supervision;
- The advisory guidelines established by resolution no. 1.1-7/172 of the Management Board of *Finantsinspektsioon* of 26 November 2018;
- MiFID II/MiFIR legislative framework.

This master's thesis is a theoretical and practical study, the result of which is a fully developed ML/TF Risk Management Framework for the process of Legal Entity verification at LEIpapa OÜ.

1. MONEY LAUNDERING AND TERRORIST FINANCING RISKS MANAGEMENT BASICS, PROCESS, AND CALCULATION

1.1. Money laundering and terrorist financing basics

The current age is the age of international control over money laundering (ML) and terrorist financing (TF) tightening. Problems related to the legalization of criminal proceeds exist not only in Estonia or any other single country. The fight against ML has become one of the global and priority problems of our time since the world has fully felt the devastating consequences of such activities on the stability and functionality of financial systems, economic growth, and public security (FATF, 2022a). The genesis of ML and TF is presented in Appendix 2. The United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, adopted in December 1988 in Vienna, was the first international instrument to address the issue of proceeds of crime and to require States to establish money laundering as a criminal offense (UNODC, 2003). The report, conducted for Swedbank by London-based law firm Clifford Chance, found that €36.7 billion in transactions, all carrying a high risk for ML, were processed through the bank's branch network in Estonia, Latvia, and Lithuania between 2014 and 2019; an estimated €4.4 billion in transactions may have violated financial sanctions imposed by the US against named Russian oligarchs suspected of ML through banks operating in the Baltic states (O'Dwyer, 2020). The estimated amount of money laundered every year is about 2-5% of global GDP, which corresponds to $800 billion to $2 trillion (UNODC, 2021) and that is one of the biggest threats to the global economy nowadays (Tiwari et al., 2020).

The "money laundering" term is derived from the argot of criminals; in common words, it is a specific process of making illegally gained proceeds (i.e. "dirty money" or "black money") appear legal (i.e. "clean" or "washed") so that they can be used openly. Typically, the process of ML involves three steps (FATF, 2022a): the first step is "placement" where illegitimate funds are furtively introduced into the legitimate financial system, the second step is "layering" where several transactions or complex financial schemes are performed to disguise the illegal source of the funds sometimes by transferring through numerous accounts, the third step is "integration" where the illegal funds are integrated into the financial system through additional transactions and benefits from the illegal funds are acquired by the criminals. In practice money laundering cases may not have all three stages,

some of them could be combined, or several stages repeat several times. As stated by Financial Crimes Enforcement Network (FinCEN), ML can facilitate crimes such as drug trafficking and terrorism and can adversely impact the global economy (FinCEN, 2021). Thus, anti-money laundering (AML) is closely related to counter-financing of terrorism (CFT), and AML regulations combine money laundering (source of funds) with terrorism financing (destination of funds).

Terrorist financing encompasses the means and methods used by terrorist organizations to finance activities that pose a threat to national and international security (UNODC, 2021). Due to the high-profile actions of proliferation actors such as the Democratic People's Republic of Korea and Iran, the financing of the proliferation of chemical, biological, radiological, and nuclear (CBRN) weapons has increasingly attracted international attention in recent years. At its core, proliferation financing focuses on the risks associated with financial products and services which are directly linked to the trade in proliferation-sensitive items (HM Treasury, 2021).

The Financial Action Task Force (FATF) is the intergovernmental body that devises and promotes international standards and methods aimed at preventing money laundering and terrorist financing. Based on the methodology developed by the FATF, the assessment of FATF countries and countries belonging to regional organizations is carried out. As a policy-making body, the FATF works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas (FATF, 2021). The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory, and operational measures for combating ML, TF, and other related threats to the integrity of the international financial system (FATF, 2022c).

Select Committee of Experts on the Evaluation of Anti Money Laundering Measures (MONEYVAL) is an expert committee of the European Council, which assesses the level of implementation of measures taken against money laundering in those Council of Europe member states that are not members of the FATF (FSA, 2021). The FATF demonstrated through several money laundering typologies exercises that ML can be achieved through virtually every medium, financial institution, or business (ACAMS, 2019, 1). A key element of FATF's efforts is its detailed list of appropriate standards for countries to implement. These measures are set out in the 40 FATF Recommendations adopted by the FATF plenary

in February 2012, with the last revision made in October 2021, which provides a complete set of countermeasures against ML and TF, covering (among others) the identification of risks and development of appropriate policies and the transparency of Legal Entities and arrangements, combined with international cooperation. At present time, all organizations of countries whose authorities do not comply with the FATF Recommendations, are not able to count on the development of international cooperation in the financial sector.

The Republic of Estonia, as a member of the European Union, must comply with the EU Directives and FATF Recommendations, respectively. First, the EU Directives are adopted, based on the requirements of the FATF, and then the EU member states implement them. By adopting the national MLTFPA law in 1997, the Republic of Estonia signed a Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime and on the Financing of Terrorism on March 7th, 2013. The Convention asks State parties for the adoption of the necessary legislative and other measures to identify, trace and confiscate the illicit property of any kind; prevent any dealing in, transfer, or disposal of such property; empower its authorities to order that – where criminal activity is suspected – bank, financial or commercial records be made available without regard to bank secrecy; legalize the use of special investigative techniques like monitoring, observation, interception of telecommunications, access to computer systems and orders to produce specific documents when criminal activity is suspected (Europe Human's Rights Watchdog, 2021).

1.2. Legal Entity Identifier and the LEI system

The LEI system was developed by the 2012 Group of Twenty (G20) in response to the inability of financial institutions to identify legal entities uniquely so that their financial transactions in different national jurisdictions could be fully tracked. Thus, the G20 endorsed the recommendations of the Financial Stability Board (FSB) regarding the framework for the development of a Global LEI system for parties to financial transactions and encouraged global adoption of the LEI to support authorities and market participants in identifying and managing financial risk (FSB, 2012b, 8). Since its introduction, the LEI has been adopted by more than one million entities across more than 200 countries (ESRB, 2020, 403/2). The Regulatory Oversight Committee (ROC) is a group of public authorities from around the globe established in January 2013 to coordinate and oversee a worldwide framework of legal entity identification, the Global LEI System (GLEIF, 2020b).

According to GLEIF, the Legal Entity Identifier (LEI) is a 20-character, alpha-numeric code based on the ISO 17442 standard (Figure 2) developed by the International Organization for Standardization (ISO). It connects to key reference information that enables a clear and unique identification of legal entities participating in financial transactions (GLEIF, 2021c).

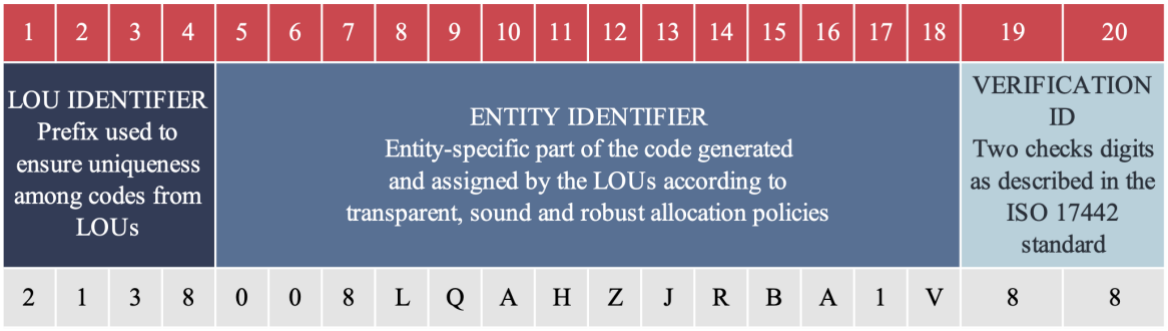


Figure 2. The meaning of the digits in the LEI code.

Source: https://docs.leipapa.com

The LEI code specifies the minimum reference data, which must be supplied for each LEI, such as the official name of the legal entity as recorded in the official registers, the registered address of that legal entity, the country of formation, the codes for the representation of names of countries and their subdivisions (GLEIF, 2021f). The information stating the date of the first LEI assignment, the date of the last update of the LEI information, and the date of expiry (when applicable) is also stored in the global database. Moreover, each LEI contains information about an entity's ownership structure (direct and ultimate parent entities) and therefore answers the questions of "who is who" and "who owns whom" (GLEIF, 2021c) for each particular entity. Every single LEI code is unique, and it shall be issued only once for a specific legal entity and the same LEI code cannot be issued to another legal entity. The LEI code does not replace the registry code (registration number of the entity) of the commercial register, which is still used to identify a legal entity.

LEI codes associate legal entities with key information, which allows them participating in global financial markets to be clearly and uniquely identified and are already used to identify the parties to EMIR derivative instruments transactions and due to the application of implementing regulation EU/2017/105, no other alternative codes can be used when providing notification of transactions made with derivative instruments starting from 1 November 2017. Moreover, LEI codes are used for reporting as of 3 January 2018. Under

the MiFIR and MiFID II (ESMA, 2018) regulation, transaction reports shall, among other things, also be used for investigating market abuse (ESMA, 2017). The total amount of LEI codes issued worldwide by February 2022 corresponds to more than two million codes (Figure 3).

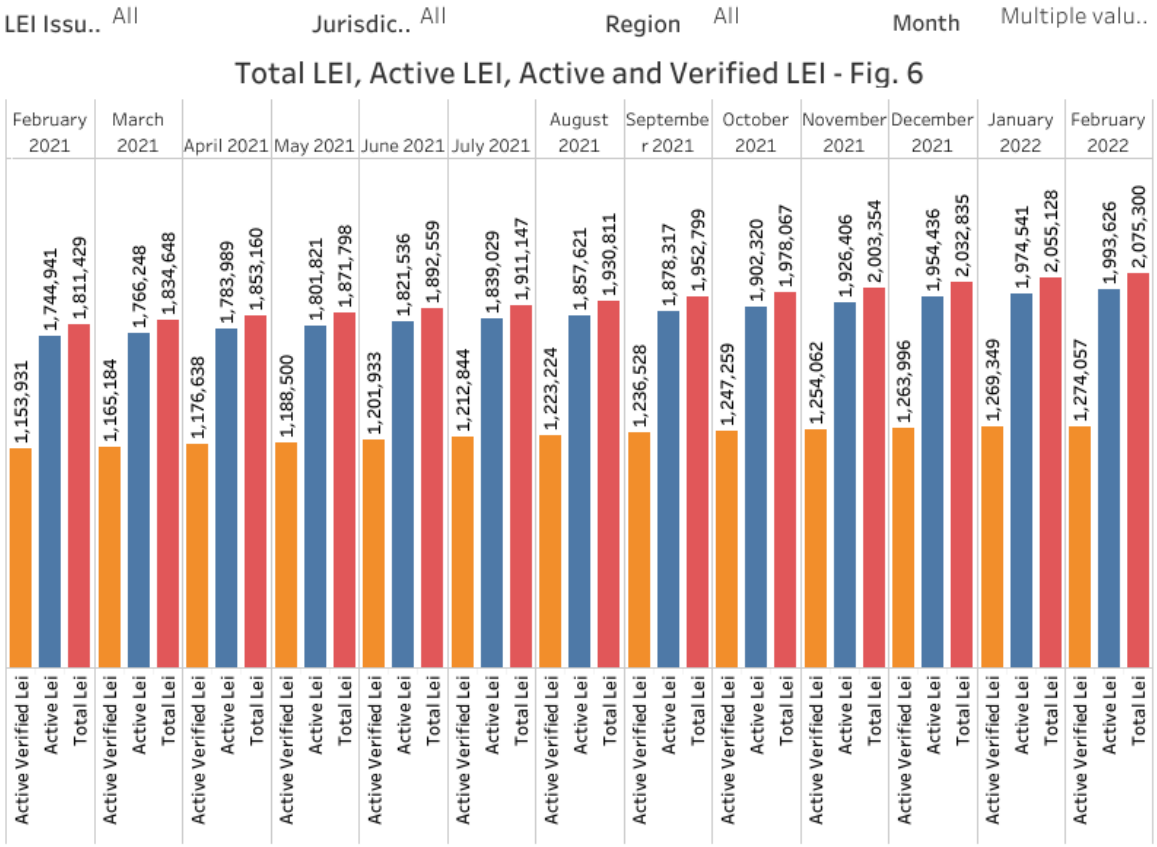


Figure 3. Total LEI, Active LEI, and Verified LEI are issued worldwide.

Source: (GLEIF, 2022c)

In simple words, the LEI code is a uniform way of keeping track of legal entities around the world (de Meijer & treasuryXL, 2019). LEI codes are global and have no borders at all for relevant and trusted identification of entities. Looking in that way, the publicly available LEI data pool can be regarded as a global directory, the registry which may greatly enhance transparency in the global marketplace. Such information is important for compliance departments of financial institutions or other obliged entities and AML specialists while conducting due diligence measures as part of their KYC procedures, especially in such cases where foreign legal entities have a complicated and opaque structure of ownership.

The management of the LEI system is coordinated and supported by GLEIF, while registrations and data storage are performed by Local Operating Units (LOUs), which, in turn, use a branched structure of Registration Agents (RAs) that receive applications from legal entities for the registration of LEI codes, checking the data, processing legal documents, sending applications to the relevant LOU for further issuance of the LEI code. GLEIF invokes that "financial services businesses can save time, gain greater transparency, and work in a more streamlined fashion by adopting an LEI for each client organization" (GLEIF, 2021e). The dynamics of LEI codes issued in Estonia from February 2021 to February 2022 are presented in Figure 4.

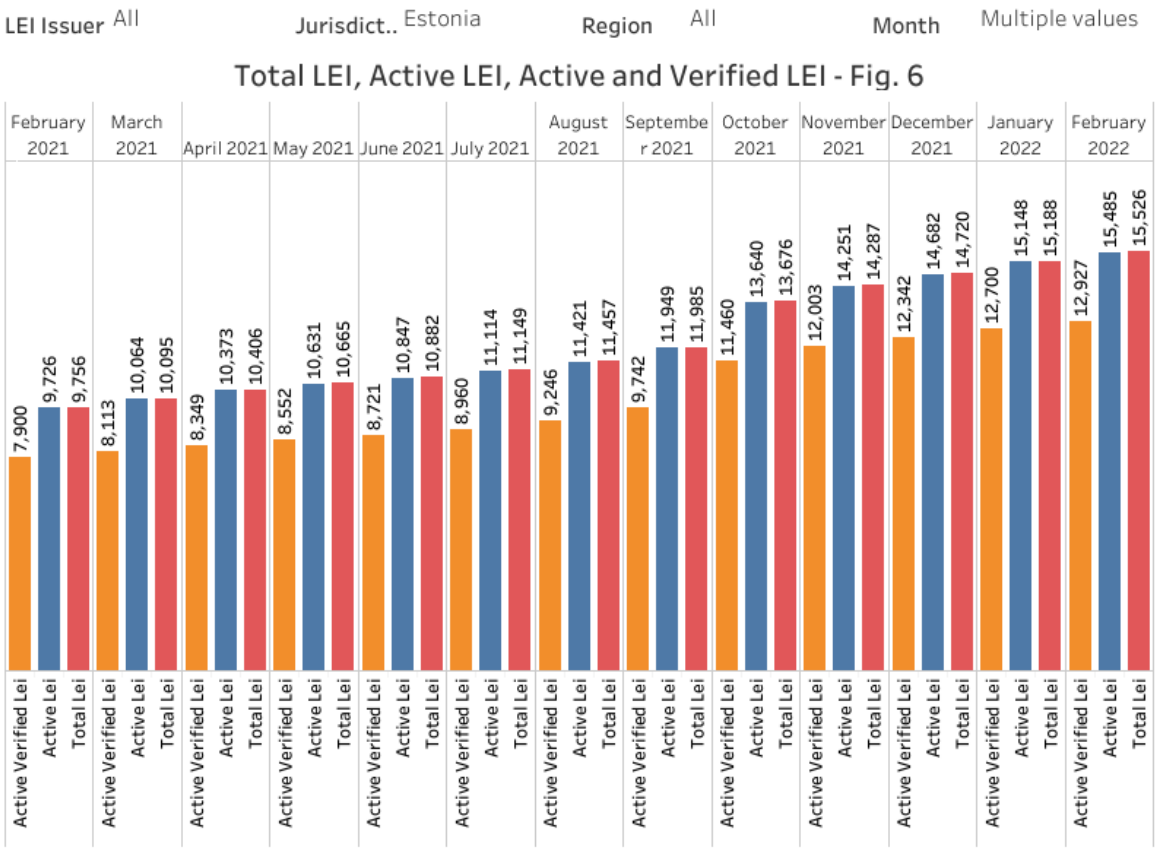


Figure 4. Total LEI, Active LEI, and Verified LEI are issued in Estonian jurisdiction.

Source: (GLEIF, 2022c)

GLEIF explores in its research (GLEIF, 2018a) the challenges that the banking sector faces when it comes to onboarding new client organizations, to investigate, in particular, the implications of Know Your Customer (KYC) requirements. Financial institutes operate in multiple jurisdictions and therefore need a global standard such as the LEI system, that offers

various businesses a unified approach to identifying legal entities, which has the potential to take the complexity out of business transactions (GLEIF, 2018a, 19).

GLEIF-specified tasks performed by a Registration Agent and the LEI issuing organizations are specified in Appendix 3; all services performed by a Registration Agent under the terms of the Registration Agent agreement concluded with the LOU are specified in Appendix 4.

1.3. Legislative basis and measures of anti-money laundering and counter-terrorist financing

The Republic of Estonia is a member state of the Council of Europe and has ratified the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (Council of Europe, 2005) which entered into force in 2008. To strengthen international cooperation and facilitate it, State parties to the Convention are obligated to establish a Financial Intelligence Unit (FIU). This term describes a national agency responsible for requesting, receiving, analyzing, and disseminating to the competent authorities suspicious financial information about suspected proceeds and potential financing of terrorism. When necessary, these units co-operate with the units of the other State parties (Europe Human's Rights Watchdog, 2021).

According to the definition from the Estonian Police and Border Guard Board and the Ministry of Finance (Ministry of Finance, 2022), the Estonian FIU is a central, independent government agency that analyses and verifies information about suspicions of ML and TF, takes measures for the preservation of property where necessary, and immediately forwards materials to the competent authorities upon detection of elements of a criminal offense.

In 2020, the Parliament of Estonia, *Riigikogu*, decided to introduce a new provision into the MLTFPA (2022, sec. 54(1), 32) entered into force on 1 January 2021, which established the principle that all obliged entities submit reports to the FIU. According to the 20th recommendation from FATF (2022b, 19), a suspicious transaction report (STR) or a suspicious activity report (SAR) is filed by an obliged entity to the local FIU if they have reasonable grounds to believe that a transaction is related to criminal activity. According to the annual report (FIU, 2021, 11), in 2020 FIU received 8,291 reports, which was an increase of more than 2,100 reports compared to 2019 (Figure 5). The number of suspicion-based reports increased significantly.

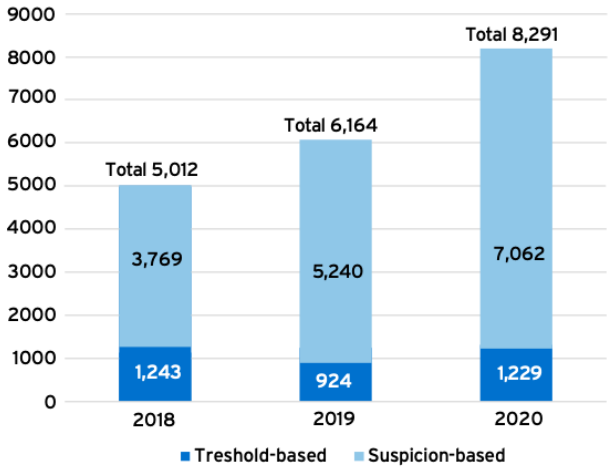


Figure 5. Reports received by the FIU in 2018-2020.

Source: (FIU, 2021, 11)

Whether or not a reported case leads to a lawsuit or other legal consequences, and thus is defined as a case related to ML or TF by the judicial power, is in principle not relevant for obliged entities. The task of obliged entities is solely to monitor all Clients and transactions passing through their system and to classify each of them as suspicious or not. It is also important to note, that for the FIU to perform its strategic analysis function, relevant data from obliged entities must be collected, analyzed, and verified via periodic reporting, thereby helping to identify methods, patterns, trends, and trends in ML and TF. The distribution of reports sent to FIU by reporting entities in 2018-2020 is presented in Table 1.

Table 1. Distribution of reports sent to FIU by reporting entities in 2018-2020

Reporting entities	2018		2019		2020	
	Reports	% of reporting entities	Reports	% of reporting entities	Reports	% of reporting entities
Credit institutions	2,208	44.1	2,905	47.1	4,594	55.4
Financial institutions	1,360	27.1	1,188	19.3	1,444	17.4
Virtual currency service providers	7	0.1	400	6.5	530	6.4
Gambling operators	279	5.6	250	4.1	118	1.4
Other obliged entities	85	1.7	75	1.2	175	2.1
Agencies and persons from other countries	541	10.8	519	8.4	585	7.1

Reporting entities	2018		2019		2020	
	Reports	**% of reporting entities**	**Reports**	**% of reporting entities**	**Reports**	**% of reporting entities**
Public agencies	266	5.3	231	3.7	284	3.4
Professionals	223	4.4	506	8.2	307	3.7
Legally non-obliged entities	43	0.9	90	1.5	254	3.1
Total	**5,012**	**100**	**6,164**	**100**	**8,291**	**100**

Source: (FIU, 2021, 13)

The Republic of Estonia also has a sanctions regime in place and follows the restrictive measures laid down by the United Nations Security Council, the European Union, and other international organizations which are binding on Estonia. International sanctions are a foreign policy tool known as restrictive measures, which aim to preserve or restore peace, prevent conflicts, strengthen international security, strengthen and support democracy, the rule of law, human rights, and fight against terrorism (Ministry of Foreign Affairs, 2021). Estonia's main legislation for enforcing international sanctions is the International Sanctions Act (ISA) (2022). The EU takes a targeted and differentiated approach to sanctions (European Council, 2022), among which are sanctions aimed at specific policies (such sanctions can target terrorism, violations of human rights, the annexation of foreign territory, etc.), sanctions focused on specific areas (diplomatic sanctions and sanctions in a narrow sense), UN and EU autonomous sanctions, sanctions with the mixed regime. The Estonian FIU is the responsible body for financial sanctions, including the freezing of funds and economic resources, financing, and financial assistance. Concerning financial sanctions, the obliged entity must notify the Estonian FIU if they know or suspect that someone with whom they are doing business, or are planning to do business, is the subject of an international financial sanction. The FIU's role in international financial sanctions is to organize state supervision of the implementation of financial sanctions in compliance with the requirements of the International Sanctions Act and to verify the legality of the measures taken by the market participant after receipt of the notification of sanctions are placed on a market participant (FIU, 2021, 35).

According to AMLD, a Directive (EU) 2018/843 (2018, sec. 30), also known as the "Fifth Anti-Money Laundering Directive", of the European Parliament and the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system

for money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, national registers of beneficial ownership information are required to be interconnected directly to facilitate cooperation and exchange of information between member states. Article 32a of AMLD (2018, sec. 32a) requires member states (Lovegrove, 2021) to put in place centralized automated mechanisms, such as central registries or central electronic data retrieval systems, which allow the identification of any natural or legal persons holding or controlling payment accounts and bank accounts to national FIUs.

1.3.1. Competent authorities of the Republic of Estonia engaged in the prevention of money laundering and terrorist financing

In the Republic of Estonia, the following institutions and entities are engaged in the prevention of ML/TF, each within the limits of their competence provided by law:

- Financial Intelligence Unit (FIU), (*Rahapesu Andmebüroo*), has primary responsibility for ML monitoring, and it collects information and observes income from criminal activities. The unit has the right to receive information from Estonian FSA and other state and local government institutions, and under an injunction from individuals, on activities, transactions, and people suspected of involvement in money laundering or terrorist financing (FSA, 2021).
- Investigative authorities (Police and Border Guard Board, Internal Security Service (KAPO), Estonian Tax and Customs Board (*Maksu- ja Tolliamet*)) actively working to identify the criminals and establish appropriate legal liabilities if necessary.
- Office of the Prosecutor General and Estonian courts (*Prokuratuur*).
- Estonian Financial Supervision Authority (FSA), (*Finantsinspektsioon*), and other supervisory authorities such as *Notarite Koda* and Estonian Bar Association (*Eesti Advokatuur*). FSA is responsible for the stability, reliability, and transparency of the financial sector of Estonia. As ML/TF financing is directly connected with the stability and reliability of the financial sector, the FSA supervises in this field as well (Ministry of Finance, 2022).
- Credit and financial institutions and other obligated persons within the meaning of the MLTFPA (*RahaPTS*).
- The Ministry of Finance (*Rahandusministeerium*) is responsible for general policy, legislation, and coordination of the activities in this area.
- The Ministry of Interior (*Siseministeerium*).

The Government Commission for the coordination of the prevention of ML/TF was established by Government Order No. 285 on 11 May 2006. The members of the Government Commission are representatives of public sector institutions and other institutions involved in the fight against ML. The Government Commission was established to set up a national coordination system, as finding an effective solution to the problems in

this area requires constant cooperation between the authorities and individuals involved. The Commission consists of representatives of the Tax and Customs Board, the Prosecutor's Office, police authorities, the Bank of Estonia (*Eesti Pank)*, and the FSA. The Commission shall meet as necessary, but not less frequently than once every four months (FSA, 2021).

In addition to local cooperation between authorities, it is also important to represent the interests of the Republic of Estonia in international committees and working groups dealing with the implementation and evaluation of the effectiveness of AML/CFT, thus the following institutions deal with the prevention of ML/TF such as Financial Actions Task Force (FATF), Select Committee of Experts on the Evaluation of Anti Money Laundering Measures (MONEYVAL), European Banking Authority (EBA), European Central Bank (ECB) and Basel Committee (BCBS), must be also noted herein.

1.3.2. Registration Agent's legislative base concerning money laundering and terrorist financing

To obtain an LEI, all information presented by the Client must be checked by the Registration Agent for data quality control purposes. Before all LEIs are issued the data is cross-checked with the local corporate registry and documentation provided by the Client's representative. The official list of company registries from which a Legal Entity can have its data confirmed is outlined by GLEIF (2019), and for Estonian jurisdiction, those registries are the Centre of Registers and Information Systems and the Estonian FSA. This ensures that the LEI is a reliable source of data and is one of the most important factors behind the LEI. The LEI system is an open-type database that is used by many persons and organizations worldwide and to ensure the database contains high-quality data, it should be sourced from a trusted registry.

By recommendation A(1) of the European Systemic Risk Board (ESRB) from 24.09.2020 on identifying legal entities, it is recommended to "propose that Union legislation incorporates a common Union legal framework governing the identification of legal entities established in the Union that are involved in financial transactions by way of a legal entity identifier (LEI), paying due regard to the principle of proportionality, taking into account the need to prevent or mitigate systemic risk to financial stability in the Union and thereby achieving the objectives of the internal market" (ESRB, 2020, 403/4). It is also stated in

recommendation A(2) to propose that Union legislation requiring legal persons to report financial information include the obligation to identify, through an LEI the legal person that is subject to the reporting requirement, and any other legal entity about which information is required to be reported and which has LEI (ESRB, 2020, 403/4).

According to MLTFPA (2022, sec. 8, p.5), the Registration Agent is defined as an obliged entity (with regards to ML/TF) and must comply with requirements specified concerning entities with the status of trust and service provider (since Registration Agent represents a Client before LOU and GLEIF), therefore, the Registration Agent shall act within the powers conferred by the regulation and within the scope of the following legislative texts:

- FATF Recommendations;
- MONEYVAL typologies;
- Anti-Money Laundering Directive (AMLD);
- Money Laundering and Terrorist Financing Prevention Act of the Republic of Estonia (MLTFPA);
- National Risk Assessment and regulations from the Ministry of Finance;
- Guidelines from Basel Committee on Banking Supervision;
- Guidelines and requirements from the Estonian Financial Intelligence Unit (FIU);
- Guidelines and requirements from the Estonian Financial Supervision Authority (FSA);
- Guidelines from European Banking Authority (EBA).

Further, the Registration Agent shall also act within the scope of all directives, regulations, and decisions based on those acts and any further legally binding EU act that confers tasks on the Registration Agent. Finally, the Registration Agent shall act according to terms of the License Agreement concluded with GLEIF and the Registration Agent agreement concluded with LOU, which is UBISECURE OY for LEIpapa OÜ. This includes matters of corporate governance, interaction, and reporting, provided that such actions by the Registration Agent are necessary to ensure the effective and consistent application of those acts.

1.3.3. ML/TF Risk Management Framework and ML/TF risks having an impact on Registration Agent

The Risk Management Framework is a template and guideline used by companies to identify, eliminate, and minimize risks (Posey, 2021a). The definition is originally developed by the National Institute of Standards and Technology of the United States, it has the main function to help protect the systems working within the organizations and was intended to

use by US federal agencies but can be readily adopted by organizations in the private sector worldwide. Organizations cannot exist without exposing themselves to risks, and obliged entities must also take care of the risk related to ML/TF. While it is impossible to eliminate all ML/TF risks associated with operating a business, they can be minimized.

Five components make up the Risk Management Framework, which includes the following (Tucci, 2021):

1. risk identification;
2. risk measurement and risk assessment;
3. risk management;
4. risk reporting and monitoring;
5. risk governance.

Let's take a closer look at each of the points above. The first component in implementing the ML/TF Risk Management Framework is to identify the ML/TF risks to which the Company is exposed and it is crucial to note that identifying risks is not a one-time process since the risks the Company faces change over time, so an ML/TF risk assessment must be conducted periodically. Risk can be defined as a combination of the probability of an event and its consequences. In simple terms, risks are a combination of the likelihood that something will occur and the magnitude of the harm or loss that may result if it does (International Organization for Standardization (ISO), 2018, sec. 3).

The goal of the ML/TF risk measurement and assessment component is to create a risk profile for each identified risk (Posey, 2021a). There are many ways organizations can complete the measurement and assessment phase of the process. The risk-based approach is central to the effective implementation of the FATF Recommendations. It is an assessment of the varying risks associated with different types of businesses, clients, accounts, and transactions to maximize the effectiveness of an AML program (ACAMS, 2019, 251). The focus on risk is intended to ensure that Registration Agent, as an obliged entity, can identify, assess and understand the ML/TF risks to which it is exposed (FSA, 2018, 9) and take the necessary AML/CFT control measures to mitigate them. Under MLTFPA (2022, sec. 13(2), p.8), the steps taken by Registration Agent to identify, assess and analyze risks must be proportionate to the nature, size, and level of complexity of the economic and professional activities, while according to MLTFPA (2022, sec. 13(1), p.8), for identification, assessment, and analysis of risks of ML/TF, the Registration Agent must prepare a risk assessment, taking into account of at least the risk categories specified below:

1. risks relating to Clients;
2. risks relating to countries, geographic areas, or jurisdictions;
3. risks relating to products, services, or transactions;
4. risks relating to delivery channels between the Registration Agent and the Client.

The risk-based approach serves as a useful tool to understand the risk areas where the associated risks are relatively high to allocate resources most effectively. As stated above, the risk-based approach recognizes that the ML /TF threats to the obliged entity vary concerning its Clients, geography, products and services, transactions, and delivery channels. It also enables the obliged entity to apply procedures, systems, and controls to manage and mitigate the identified ML /TF risks and facilitates the allocation of resources and internal structures to manage and mitigate the identified ML /TF risks. The risk-based approach provides threat and vulnerability assessment of the obliged entity used as a channel for ML /TF. By regularly assessing the ML/TF risks, the obliged entity can protect and maintain the integrity of its business and the financial system as a whole. Moreover, an obliged entity using a risk-based approach must proactively seek information on ML trends and threats from external reliable sources, such as law enforcement, and rely on its own experience and observations. In this way, the obliged entity can effectively review and revise its use of AML tools to match the specific risks it faces.

The third component of the ML/TF Risk Management Framework is risk management. Risk management is a systematic process of examining the identified risks and determining which risks can and should be eliminated (also, which risks are considered acceptable), developing methods to minimize and manage risks, and such process requires developing a method to identify, prioritize, address (deal with), control, and monitor risks (coordinated activities to direct and control an organization concerning risk) (ISO, 2018, sec. 6.4).

The author describes below the process of risk score calculation and risk assessment for the obliged entity based on the information provided in CAMS Study Guide (2019, 142–149). Risk management involves a process of evaluating risks in terms of the likelihood (opportunity) of their occurrence and the severity or amount of loss or damage (impact) that may occur if they do occur. Therefore, each risk element can be rated by:

- Likelihood - the chance of the risk happening.
- Impact (consequence) - the amount of loss or damage if the risk happened.

Thus, it is possible to apply the risk rating scales for likelihood and impact, and from those results get a risk level or risk score using the risk matrix and the formula:

$$Likelihood \times Impact = Risk\ level\ (Risk\ score)$$

A likelihood scale refers to the potential of an ML/TF risk occurring in the Company for the particular risk being assessed. Table 2 below lists three risk levels, but the Company may set as many levels as it deems necessary.

Table 2. Likelihood scale

Frequency	Likelihood of ML/TF risk
High likely	It will probably occur several times during a relevant timeframe
Likely	Highly probably it will happen once during a relevant timeframe
Unlikely	Unlikely, but not impossible at all

Source: CAMS Study Guide (2019, 142–149), compiled by the author

An impact scale refers to the severity of the harm that might (or might not) occur if the risk were to occur. When evaluating the possible impact or consequence, the evaluation can be done from different points of view. It does not cover everything and is not prescriptive. The impact of an ML/TF risk may be assessed or considered from the following perspectives, depending on the Company and its business model. Table 3 below shows three levels of impact, but the Company can have as many as it deems necessary.

Table 3. Impact scale

Consequence	Impact of ML/TF risk
Major	Huge consequences – major damage or effect. Case of serious ML/TF
Moderate	Moderate level of ML/TF impact
Minor	Minor or negligible consequences or effects

Source: CAMS Study Guide (2019, 142–149), compiled by the author

While using the risk matrix to combine likelihood and impact to obtain a risk score, the risk score can be used as a decision-making tool to help decide what action to take in a particular case given the overall risk. There are four levels of risk score considered in this case, but the Company can set as many levels as it deems necessary, and the risk matrix (Figure 6) shows how the risk score is derived.

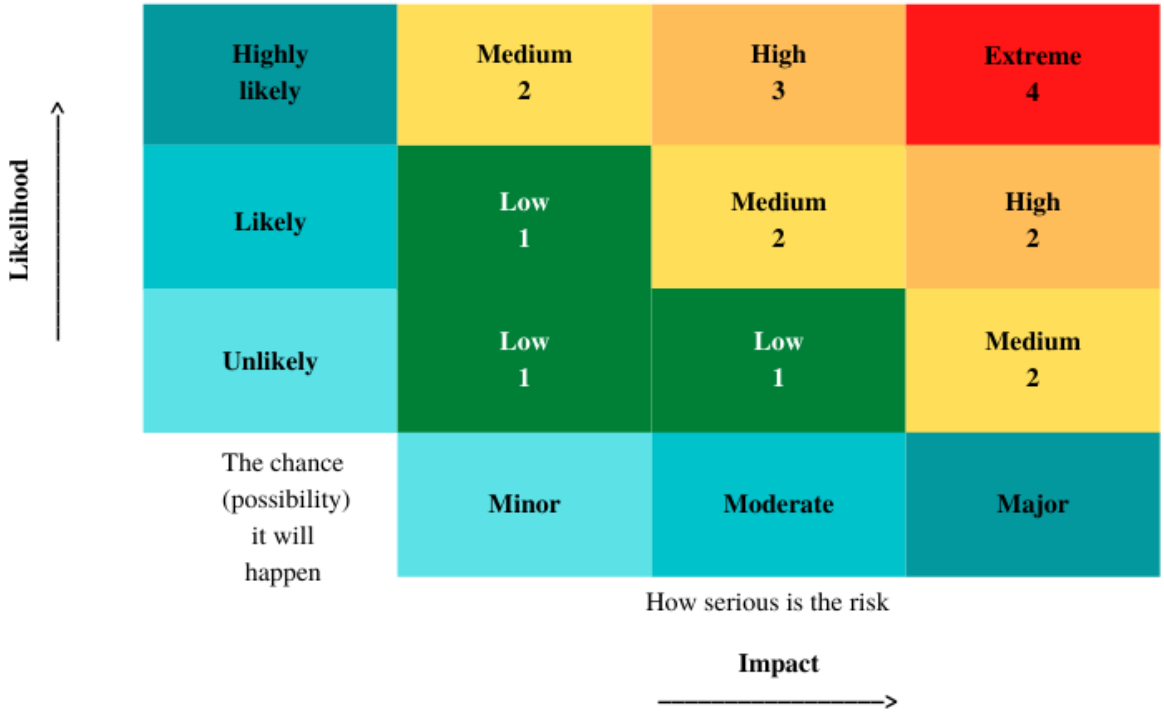


Figure 6. Risk matrix.

Source: CAMS Study Guide (2019, 142–149), compiled by the author

The risk score has the following gradation here (Table 4):

Table 4. Risk score

Rating (score)	Impact of an ML/TF risk	Response
4 – Extreme	Risk almost sure to happen and/or to have very dire consequences	Business relations are not allowed
3 – High	Risk likely to happen and can have serious consequences	Conduct enhanced due Diligence (EDD). Do not allow business relations/transactions until the risk is reduced
2 – Medium	The risk could happen and/or have moderate consequences	Conduct customer due diligence (CDD). Possible to proceed with business relations/transaction but preferably reduce risk first
1 – Low	Unlikely to happen and/or have minor or negligible consequences	Conduct simplified due diligence (SDD). Free to proceed with business relations/transaction

Source: CAMS Study Guide (2019, 142–149), compiled by the author

For the aspects of ML/TF, Registration Agent expects risk management to consider two main risks: business risk and compliance risk.

Business risk is the risk that the Registration Agent could be used for ML/TF (HM Revenue & Customs, 2021). Such risk includes the risks that have already been mentioned above (risks relating to Clients, risks relating to countries, geographic areas, or jurisdictions, risks relating to products, services, or transactions, risks relating to delivery channels between the Registration Agent and the Client).

Compliance risk is the failure of the Registration Agent to comply with all obligations arising from FATF Recommendations, AMLD, MLFTPA, and other relevant regulations and guidelines. Often, compliance risk results from insufficient control systems, lack of training, lack of due diligence, and human error (nibusinessinfo, 2021). Examples of regulatory obligations that may be breached include reporting SAR and STR, verifying the identity of the Clients, and having an AML/CFT program.

The compliance risk can potentially expose the Company to a damaged reputation and loss of business opportunities, and nowadays organizations are exposed to a greater degree of compliance risk than ever before (Deloitte, 2015, 1). The occurrence of the compliance risk event can lead to the event of ML (for example, in case of inactivity of the employee of the Registration Agent, issues in workflows, etc.), and as a consequence, the fine may be applied to the Registration Agent in the amount up to €400.000 (MLTFPA, 2022, Chapter 10, secs. 82-96, pp. 53-55) or the responsible employee of Registration Agent in the amount up to 300 fine units. In several cases it is also possible such violation can lead to the breach of the License Agreement concluded with GLEIF, and therefore the license of the Registration Agent can be withdrawn.

The fourth component of the ML/TF Risk Management Framework is risk reporting and monitoring. This essentially means reviewing risks regularly to ensure that the risk management and mitigation strategies the Company has adopted are having the desired effect. Risk reporting is a method of identifying risks that are associated with or could impact the Company's business processes. Identified risks are typically summarized in a formal risk report, which is then communicated to senior management or various management teams within the Company (Posey, 2021b).

Risk governance is the final component of the ML/TF Risk Management Framework and is designed to ensure that the adopted risk management and mitigation techniques are implemented in the Company and that employees adhere to the policies.

1.4. Fundamentals of the ML/TF risk management in the Republic of Estonia

The Estonian financial sector has zero-tolerance for ML/TF, which means that obliged entities in Estonia must be law-abiding, comply with all legal acts governing the field, abide by international best practices, standards, and guidance of FATF, the Basel Committee, Financial Crimes Enforcement Network (FinCEN), local bodies such as Estonian FSA and Estonian FIU, and other appropriate bodies. To achieve the objective of this study and develop a complete ML/TF Risk Management Framework, it is necessary to understand that the Company can't operate in a completely ML/TF risk-free environment. Thus, the Company should identify the ML/TF risk it faces and then works out the best ways to reduce and manage that risk. It is also necessary to understand the core of the Risk Management Framework which consists of the risk management model that takes into account IT and human resources that need to hedge the risks and threats while identifying and verifying Clients. When needed, an obliged entity should recruit additional experts and conduct investments for raising competence and developing, or integrating, existing risk-sensitive and adequate IT systems. The adequacy of such systems, and the control systems as a whole, must be assessed regularly to be sure that the risk management model is functioning properly and in full accordance with the existing laws and regulations.

To manage the factors of compliance risk, it is necessary to specify the main principles of the management in the Company and develop a complete framework for managing the ML/TF risks by the existing laws and best practices, i.e., functional organizational structure and clear internal procedures, where the processes and the workflow of the Company are specified. It is also necessary to mention additional principles needed for the proper functioning of the Framework.

1. Carry strict subordination with the management of the Company.
2. Prepare an ML risk assessment for Company's operations based on a risk-based approach.
3. Submit a notice on any suspicious business activity (SAR) or transactions (STR) to the FIU.
4. Ensure that the obligations of the Company under the MLTFPA are well-known and that employees can observe them in their everyday operations, continuously developing their knowledge.
5. Identify and know Clients (KYC) and track their activities.
6. Provide responsible employees with sufficient financial, human, and technical resources with sufficient authority to carry out their functions.

One of the important aspects of the functioning of the Framework may be the presence of a sole executive body in the person of the Member of the Board of the Company, which is responsible for compliance with the current legislation and determines the risk appetite of the obliged entity. Everyone should report directly to the Member of the Board of the Company, who determines the strategy and goals of the Company, recruits, supervises their activities, and provides internal control. The Board Member appoints a compliance officer responsible (a contact person) for the implementation of internal procedures aimed at AML/CFT. The role that the compliance function plays within a Company is evolving as business strategies, regulatory requirements and societal expectations continue to develop. A well-functioning compliance team is a key element of any successful Company (Deloitte, 2021, 5). Cooperation of the employees within the Company workflow leads to a proper choice of a set of measures to reduce the risk of ML/TF.

The Company applies due diligence measures, by the Interpretive Notes to FATF (2022b) Recommendation 10 (2022b, 64-72) and FATF Recommendation 1 (2022b, 31-36), to ensure the quality and smoothness of communication with Clients, that the relevant data are gathered and the requirements are clear for Clients. For this purpose, the Company must train employees concerning diligence measures and provide sufficient guidance regarding communication with Clients, ensuring that employees on the first and second line of defense undergo regular training, as well as getting updates in the field of international financial sanctions. This approach ensures the high quality of service and proportionality of necessary data collection.

The Company is also obliged to enable employees to file anonymous reports on suspected violations of the MLTFPA both in the Company, share such information to external authorities via their channels through which reports can be submitted anonymously, constantly train employees and explain the opportunities and goals of whistleblowing. When necessary, a Board Member of the Company should apply a set of measures to protect Company employees who fulfill a notification obligation under MLTFPA (in the Company or by sharing the information directly with FIU), as well as other employees, from threats and hostile action from Clients and any other discriminatory treatment.

The Company, acting as an obliged entity under MLTFPA, must know its Clients and perform ongoing monitoring of the Client relationship. When the unusual transaction is

spotted, the responsible employee must perform enhanced checks, and if the transaction appears suspicious even after the investigation, report it immediately (within two working days after identifying the activity or facts or after getting the suspicion) to the Estonian FIU under MLTFPA (2022, sec. 49, p.29). The obligation to send a report to FIU is also applied each time the Company suspends a business transaction due to having suspicions.

The ML/TF risk assessment program determines the procedures for assessing and assigning a degree (level) of risk to a Client, taking into account the requirements for its identification in the event of a contractual relationship with the Client (accepting him for service); in the course of customer service (as operations (transactions) are performed); in other cases provided for by the Company in the rules of internal control. The program provides carrying out a risk assessment of Clients based on signs of transactions, types, and conditions of activity that have an increased risk of Clients performing transactions for ML/TF by the FATF Recommendations (Кононова et al., 2016, 185).

As mentioned before, under MLTFPA (2022, sec. 13(1), p.8) it is necessary to understand the risks associated with Clients, either individually or as a category, and the structure of the Client portfolio, taking into the account following factors (HM Revenue & Customs, 2021):

- new Clients carrying out large, one-off transactions or involved in a business that handles large amounts of cash;
- a Client who's been introduced to the Company - because the person who introduced them to the Company may not have carried out due diligence measures thoroughly;
- Clients who are not local to the business of the Company;
- Clients who are PEP or related to PEP in any way;
- Clients with a complicated ownership structure that could conceal underlying beneficiaries;
- Clients who make regular transactions with the same individual or group of individuals.

Client's behavior that may indicate a potential risk (HM Revenue & Customs, 2021):

- the Client doesn't allow identification, or gives the Company identification that is not satisfactory;
- the Client's representative or attorney doesn't want to reveal the name of a person they represent;
- the Client shows that they agree to bear very high or uncommercial penalties or charges;
- the Client enters or performs the transactions that do not make commercial sense at all, or in their business industry;

- the Client is involved in transactions where the Company cannot easily check where funds have come from.

Risks associated with products and services mean that inappropriate assets could be placed in the business of the obliged entity, or moved from or through it from a product or service which allows the ownership of assets to be disguised when the obliged entity supplies services without meeting a customer face to face. Such areas of activity can be considered to be (Eesti Pangaliit, 2022, 8):

- providers of virtual currency services;
- e-money institutions and payment service providers;
- crowdfunding platforms;
- companies that operate in other fields and create possibilities for rapid and simplified transactions with monetary value and concerning which there is no established regulatory framework and supervision.

Since its inception, FATF has had a practice of marking the countries that it determines to maintain inadequate AML controls or are not cooperating in the global AML/CFT efforts (ACAMS, 2019, 99). FATF's Public Statement (2019) identifies countries or jurisdictions for which the FATF calls on its members to apply enhanced due diligence measures proportionate to the risks arising from the deficiencies associated with the country; according to the report of the European Banking Authority (2021, 18), jurisdictions associated with higher ML/TF risk means countries that, based on an assessment of the risk factors set out in AMLD (2018, sec. 9(2)), and obliged entities should ensure that they apply, as a minimum, the enhanced due diligence measures set out in AMLD (2018, sec. 18a(1)) and, where applicable, the measures set out in AMLD (2018, sec. 18a(2)). The Company must also check for the information available that the Client, or their counterparty, or counterparty's bank, are registered or performing an activity on the territory of a country, to which international sanctions applied or such entity included in the so-called "black-list" of international organizations. In regards to sanctions, the Company should act by the provisions of the International Sanctions Act (ISA) of the Republic of Estonia, which, under the ISA (2022, para. 1(1)), "regulates the national imposition of international sanctions, the implementation, and the supervision thereof where the imposition of international sanctions has been decided by the European Union, the United Nations, another international organization or the Government of the Republic". The sample table of risk factors is presented below (Table 5).

Table 5. Risk factors and illustrative measures

Customer base	Products, services	Delivery channels	Jurisdictions	Qualitative factors
• Legal form, ownership structure • Length of relationship • PEP status • Industry • Customer Risk Rating (CRR)	• High degree of anonymity or limited transparency • Rapid movement of funds • High volume of currency or equivalents • Payments to/from third parties	• Account origination • Account servicing	• Location of business • Location of Clients • Origin or destination of transactions	• Growth vs. stability • Mergers and acquisition • Strategy changes • New regulatory requirements • Emerging risks

Source: (International Finance Corporation (IFC), 2019, 21)

It is also important to consider the internal environment within the Company when understanding ML/TF risk factors, as well as the efficiency of the internal procedures implemented for compliance with the MLTFPA. Technology can be an important factor in an effective compliance program, but it is not a panacea and must be used appropriately (Deloitte, 2015b, 9).

Following FATF guidance, the Company should implement risk-based due diligence measures that reflect the specific level of ML/TF risk that each Client pose. This is the way for the Company to align the compliance obligations with the Company's budget and resource requirements and preserve the experience of interaction with the Client. Based on the risk assessment, the Company determines the situations and conditions whereby the obliged entity may apply enhanced or simplified due diligence measures in economic activities and defines the content and essence of enhanced or simplified due diligence measures (FSA, 2018, 10). Examples of enhanced and simplified due diligence measures are specified in Table 6 below.

Table 6. Examples of enhanced and simplified due diligence measures

Enhanced due diligence (EDD)	Simplified due diligence (SDD)
Obtaining additional information on the customer (for example, occupation, the volume of assets), and updating more	• Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (for example,

Enhanced due diligence (EDD)	Simplified due diligence (SDD)
regularly the identification data of the customer and beneficial owner. • Obtaining additional information on the intended nature of the business relationship. • Obtaining information on the source of funds or source of wealth of the customer. • Obtaining information on the reasons for intended or performed transactions. • Obtaining the approval of senior management to commence or continue the business relationship. • Conducting enhanced monitoring of the business relationship by increasing the number and timing of controls applied and selecting patterns of transactions that need further examination.	if account transactions rise above a defined monetary threshold). • Reducing the frequency of customer identification updates. • Reducing the degree of ongoing monitoring and scrutinizing transactions based on a reasonable monetary threshold. • Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship but inferring the purpose and nature from the type of transactions or business relationship established.

Source: (FATF, 2022b), excerpts compiled by the author

Thus, an effective due diligence process should include the following steps:

- before entering into a business relationship, the Company should determine the identity and business activities of the new potential Client;
- once a Client with a sufficient level of trust has been identified, the Company should categorize the risk level of the Client. This information should be stored in a digitally secure location where it can be easily accessed for future regulatory review (i.e. request from FIU) for no less than five years according to MLTFPA (2022, sec. 47, pp.27-28).
- once a risk category has been determined, the Company should decide whether more intensive enhanced due diligence measures are required.

The Client's risk rating (risk level) assists the Company in its decision to enter, continue, or terminate the business relationship and determines the extent of controls that must be in place to manage the ML/TF risk, including the nature of ongoing monitoring of suspicious activity. An example of the Client's risk rating is presented in the table below (Table 7).

Table 7. Client's risk rating

Risk category	Examples of risk measures
Customer's demographics	Employment classification and occupation Visa status PEPs

Risk category	Examples of risk measures
	Length of relationship Industry Entity type/Ownership structure
Products/Services/ Channels	High-risk products or services High volume/value of cash/monetary instruments High volume/value of wires to/from high-risk countries
Geographies	Customer location Location of customer's operations/assets Country of incorporation Nationality Citizenship
Other factors	Country/regulatory risk Customer's AML/CFT program Negative news/regulatory action Previous compliance history (alerts, investigations, suspicion transaction reports, internal watch list)

Source: (International Finance Corporation (IFC), 2019, 29)

It is important to note there are no unified procedures for ML/TF risk assessment in Estonia and/or any other EU country. Every obliged entity is responsible for the development of rules of procedure and internal rules according to MLTFPA (2022, sec. 14, pp.9-10), AMLD, and FATF Recommendations, using a risk-based approach. AMLD puts the risk-based approach at the center of the EU's AML/CFT regime; recognizes that the risk of ML/TF may vary between countries, sectors, and financial institutions and that the Member States, competent authorities, and obliged entities should identify and assess these risks to decide how to best manage them (EBA, 2021b, 3). This approach implies that higher-risk Clients, higher-risk products, or other factors may necessitate more stringent controls and ongoing monitoring (IFC, 2019, 24). A risk-based approach is a relevant concept since it is mentioned in the MLTFPA, and international standards use the concept of a risk-based approach, i.e., determination of possible losses of obliged entity, which can lead to fines and the withdrawal of license for noncompliance with MTFPA. The current risk assessment system of the Registration Agent is to be reviewed in the following chapter.

2. OVERVIEW AND ANALYSIS OF RISK ASSESSMENT SYSTEM OF REGISTRATION AGENT LEIPAPA OÜ

2.1. Overview and main characteristics of LEIpapa OÜ

LEIpapa OÜ is an organization established on August 02, 2021, by the legislation of the Republic of Estonia under registration code 16283000.

From August 04, 2021, LEIpapa OÜ is the official Registration Agent by the license agreement concluded on August 04, 2021, with the Global Legal Entity Identifier Foundation (GLEIF), as well as the terms and provisions of the Registration Agent agreement concluded on August 04, 2021, with UBISECURE OY (Finland), an LEI issuer, branded as RapidLEI, acting according to a master agreement with the Global Legal Entity Identifier Foundation (GLEIF) dated October 10, 2016.

There are three persons working at the moment for the LEIpapa OÜ, which are its shareholders, two of them also hold the position of Board Member of the Company. In addition, LEIpapa OÜ has concluded telework agreements with two employees, one of them performs the duties of a compliance officer, while the second one combines the duties of a compliance officer and depositary.

The Company is in its first year of operation and, to date, has financial data only for the months in which services are rendered to Clients. However, LEIpapa OÜ has a very simple work structure with a clear business model, as it provides services to its customers at fixed prices, has a fixed cost, and is not involved in the trade of goods. Thus, it is very easy to perform analytical forecasts and make calculations regarding the performance of LEIpapa OÜ for the current and the next year.

As mentioned in Appendix 4, among other tasks, the Registration Agent must perform data collection or aggregation services from the relevant authoritative sources and validate the legal Reference Data provided by a Legal Entity that wishes to obtain an LEI. The possibility of high-quality execution of tasks above strongly affects both the strategy of the Company as a whole, and all business processes occurring in the Company.

One of the main strategic goals for LEIpapa OÜ is to achieve in 2023 the title of the largest Agent for LEI issuance in terms of service volume in the Baltic States.

Due to its youth, LEIpapa OÜ is at the bottom of the rankings in the Estonian market, both in terms of the total volume of LEIs processed to new Clients and in terms of Clients transferred from other Registration Agents. The share of the Company is less than 2%, but, judging by the indicators of several months, this position will change significantly in 2022, which indicates the outstripping growth of the Company in the overall market growth. The main competitors of LEIpapa OÜ are LEI Register OÜ and Baltic LEI OÜ, which together occupy about 98% of the LEI market in Estonia. The current market share of the Company is presented in the table below (Table 8).

Table 8. Market share of LEIpapa OÜ and its competitors

Name	Reg. code	Reg. date	Taxable Turnover 3q. 2021, €	Market share %	Taxable Turnover 4q. 2021, €	Market share %
LEI Register OÜ	14412769	22.01.2018	€1 413 011,00	53.6	€2 741 926.07	59.58
Baltic LEI AS	14357869	24.10.2017	€1 185 218,00	44.96	€1 810 520.16	39.34
LEIpapa OÜ	16283000	02.08.2021	€37 280,00	1.41	€46 918.14	1.02
VP Markets OÜ	12306661	27.06.2012	€750,00	0.03	€2 576.72	0.06

Source: Compiled by the author with the public data available

As can be seen from the table above, LEIpapa OÜ captured two percent of the market in just two quarters. These indicators are a very good start for the Company and suggest an offensive strategy in the future, not only within the market of the Republic of Estonia but also within the entire Baltic region. For its successful implementation, the Company will need resources that need to be prepared from the beginning of the activity. The Company aims to conquer the market of the Baltic countries, and this will require additional financial investments and the use of modern technological resources. The Company's management decided to pursue a cost minimization strategy, which should result in the accumulation of financial resources for the implementation of modern technological solutions that allow

providing an exclusive service in terms of quality and speed to Clients, which will allow the organization to successfully attack competitors and enter new markets.

The IDEF0 diagram presented in Appendix 5 displays the main and service processes of the Company, inputs, outputs, control actions, and devices interconnected with the main functions. The main process of LEIpapa OÜ is the process of verifying the Client's documents for subsequent registration with the issuance of an LEI identifier.

In the author's previous research work (Jefremov & Makhmudov, 2021, 35), the factors having the most significant impact on the performance of the Company's business processes were systematized and their expert assessment was carried out; the principles for the introduction of an automated verification system were proposed, suggesting the rationale for the need to introduce an automated technical means suitable for customer identification and verification. Authors performed the determination of the volume and sources of financing, identification of risks associated with the introduction of an automated system, and assessment of the impact of an automated system on the efficiency of business processes in the Company. Based on the results of the research work, the author concluded that the introduction of an automated verification system is economically feasible since the payback of the automated system is expected within the first year of its use in the Company. At the same time, the effectiveness of the business processes operating in LEIpapa OÜ increases in terms of several indicators.

2.2. Risk assessment system of LEIpapa OÜ

Under MLTFPA (2022, sec. 13(1), p.8), LEIpapa OÜ is required to prepare a risk assessment to identify, assess and analyze the risks related to ML/TF associated with its activities. At the moment several different entity types are eligible for LEI applications, among which are a Legal Entity, a trust, a fund, a will/pension, and other corporate entities. The full list of document requirements for the LEI application is presented in Appendix 6. The Company currently analyzes the data obtained during the implementation of due diligence measures by its "Rules of Procedure for Monitoring Money Laundering and Terrorist Financing and Compliance with International Sanctions" (Appendix 7), which only address the risks associated with the Client. That means the Company should explain and state in the risk assessment what are the higher and lower risks due to the nature of its business that may be

used for ML. By MLTFPA (2022, sec. 13(1), p.8), LEIpapa OÜ should prepare a risk assessment taking into account at least the following risks categories:

1. risks relating to Clients;
2. risks relating to countries, geographic areas, or jurisdictions:
3. risks relating to products, services, or transactions;
4. risks relating to communication, mediation or products, services, transactions, or delivery channels between the obliged entity and customers;

compare the data obtained with risk factors identified for each ML/TF risk category and determine the Client's risk profile accordingly.

According to the latest FATF report (2022d, 28–29), designated non-financial businesses and professions mostly have a below-average to poor understanding of risk related to ML/TF and more than 70% of countries are poorly implementing mitigation measures. It is also stated in the report that in most sectors, obliged entities do not file risk-based suspicious transaction reports (STRs), and that is particularly a problem for businesses and professionals outside the financial sector. The FATF analysis showed that only 6% of trust and company service providers reported suspicious transactions in a manner consistent with the country's risk profile. The relevant figures are presented in Appendix 8.

The model currently used in the Company for identifying the Client's risk profile is based on the least requirements of regulators for the companies acting as providers of trust and company services (MLTFPA, 2022, sec. 8, p.5). Using such a model it is not possible to identify unusual transactions and anomalies in business relationships that may indicate ML/TF, while the FATF points out that trusts and company service providers must focus their efforts on preventive measures and "strengthen their reporting requirements on suspicious transaction reports" (FATF, 2022d, 30).

The risk profile should demonstrate the Company's risk tolerance parameters to the four key risk categories mentioned above for any given business relationship. Each Client's risk profile is compared to the Company's risk profile as a way of assessing whether such Client falls within the agreed risk appetite of the Company. The author shows below a sample of how for the each of aforementioned risk categories the risk score may be identified:

1. Low risk – There are no influential risk factors in the risk category, the Client (representative of the Client, or Beneficial Owner) and its activities are transparent and do not deviate from the usual activities, i.e., the activities of a reasonable and

average person in this area of activity, and there is no suspicion that the risk factors as a whole could lead to the realization of the ML or TF risk.
2. Medium risk – There are one or more risk factors in the risk category that deviate from the usual activities of a person in this area of activity, but the activity is still manageable and there is no suspicion that the risk factors, taken as a whole, could lead to the realization of the ML or TF risk.
3. High risk – There are one or more risk factors in the risk category that, taken together, raise suspicion that there is a lack of transparency of the Client's (Client representative's, or Beneficial Owner's) activities, resulting in the deviating from those typically engaged in the activity and making it at least possible that ML or TF will occur.
4. Prohibited risk – The risk is unacceptable to the Company based on the risk appetite.

Each risk category is scored based on risk factors identified for the scoring Client. The score for the risk category can be determined by the higher score of the identified risk factor in the risk category. The risk score of each risk category can be used in the table presented in Appendix 9 to determine the overall Client's risk profile. Besides, the Company should also prepare an organizational solution for the prevention of ML/TF based on the principle of three internationally recognized lines of defense under Advisory Guidelines (FSA, 2018, 13-19).

2.3. Possibilities of using technical means for Client's verification

In this clause, the author clarifies the application of FATF Recommendation 10 (a) (2022b, 14) in the context of technical means for the Client's verification, which states that AML obliged entities when establishing business relations (i.e., during the onboarding process) are required to identify the customer and verify the customer's identity, "using reliable, independent source documents, data or information" (FATF, 2022b, 14) which does not impose any restrictions on the form (physical or digital) that identity evidence can take. An AML obliged entities are required to determine the extent of customer due diligence measures using a risk-based approach following the Interpretive Notes to FATF Recommendation 10 (2022b, 64), which is neutral to methods and techniques of identification and verification, and FATF Recommendation 1 (2022b, 10). Thus, there are no requirements in the FATF standards for how a verified customer identity should be linked to a unique, real person as part of the identification/verification process during onboarding, and, therefore, there are no restrictions on the use of technical means for this purpose.

Reliability is useful in determining whether a particular IT system provided by a third party is "reliable and independent" for AML purposes, which means that such a system is based

on technology, appropriate governance, processes, and procedures that provide a reasonable level of confidence in the accuracy of the system's results.

FATF Recommendation 10 (2022b, 64) requires regulated entities to use a risk-based approach (RBA) to determine the scope of customer due diligence measures to be applied, including customer identification and screening. As already stated in clause 1.4. of this thesis, an AML obliged entity is required to identify, assess, and take effective action to mitigate ML /TF risks (for customers, countries, or geographic areas; products and services, transactions, delivery channels). Increased measures are required in higher-risk situations and simplified measures may be appropriate in low-risk situations. The Interpretative Note to FATF Recommendation 10 (2022b, 64) mentions business relationships or transactions that are performed not face-to-face (not in the same physical location) as an example of a situation with potentially higher risk when conducting customer due diligence. While this statement does not require an obliged entity to always classify business relationships that do not take place face-to-face as a higher risk for ML/TF, such relationships are examples of circumstances in which the risk of ML/TF may potentially be higher and that should be considered by the Company when determining the Client's risk rating.

Following FATF Recommendation 17 (2022b, 18), AML obliged entities may rely on third parties for identification and verification of customers during the onboarding process when such third party is also an obliged entity that is subject to customer due diligence requirements according to FATF Recommendation 10 (2022b, 14) and is supervised or monitored for compliance. Moreover, the third party must comply with the local legislation of the obliged entity and with data retention requirements following FATF Recommendation 10 and FATF Recommendation 11 (2022b, 15).

Regarding ongoing monitoring, the IT system provided by third-party should allow an obliged entity to determine its criteria for additional monitoring, suspicious transaction reporting (STR), or other steps to mitigate risk (BCBS & BIS, 2020, 30), while the compliance officer should have access to and benefit from the IT system as relevant to his or her function. FATF (2020, 8) proposed a flowchart for the decision process that provides a path for obliged entities to decide whether to use a technical means for customer identification and verification and ongoing due diligence (Figure 7).

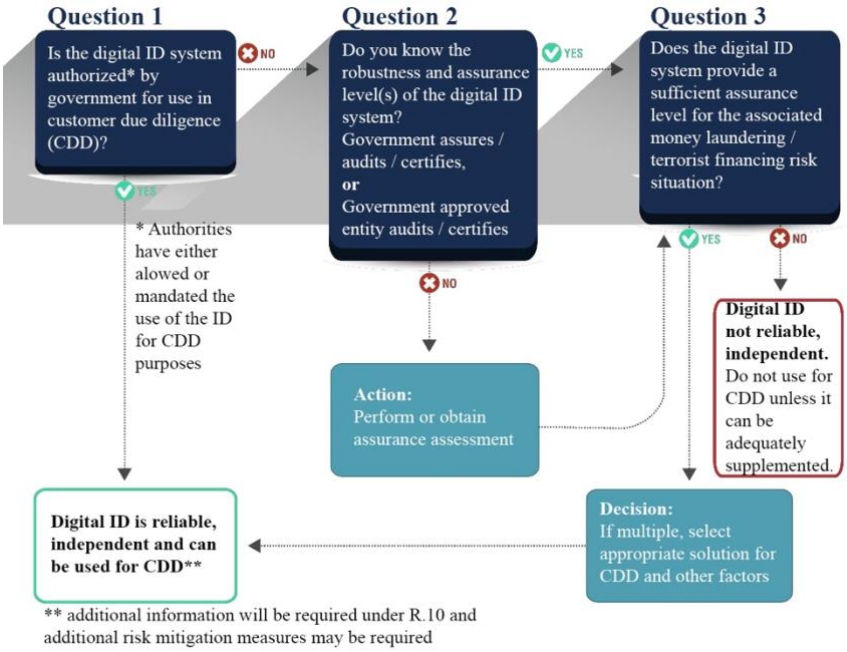


Figure 7. The decision process for obliged entities.

Source: (FATF, 2020, 8)

Among the potential benefits of using technical means for the Clients' identification and verification, FATF lists the strengthening of customer due diligence, avoiding weaknesses in human control measures, improving customer experience, generating cost-saving, performing ongoing monitoring, and the financial inclusion (FATF, 2020, 35–38).

As stated by *Eesti Pangaliit* (from the Estonian meaning "Bank of Estonia") (2022a), in the case of authentication with the tool IT, the quality of the information flow and the information system itself is subject to the requirements set out in a regulation issued by the Minister of Finance. Such regulation known as "Requirements and procedure for identification of persons and verification of person's identity data with information technology means" (Minister of Finance, 2018) is established based on the MLTFPA (2022, sec. 14(8) p.10, sec. 31(6) p.20). In addition to the FATF requirements, according to Estonian regulation (Minister of Finance, 2018, sec. 2(2) p.1), the Client "must use a document intended for the digital identification of a person and issued based on the Identity Documents Act or other high-confidence e-identification systems, which has been added to the list published in the Official Journal of the European Union based on Article 9 of Regulation (EU) No 910/2014 of the European Parliament and the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive

1999/93/EC (OJ L 257, 28.8.2014, pp. 73–114), and an information technology means, which has a working camera, microphone, the hardware and software required for digital identification and an internet connection of adequate quality" (2018, sec. 2(2) p.1). The information above means that it is not possible to perform an offline identification and verification if the Company wants to have such processes to be equivalent to verify a customer's identity face-to-face. In any case, the KYC requirements must be met, and the person behind the Client must fill out a form and answer questions from the Company in the form of a direct conversation (Eesti Pangaliit, 2022a). Among the technical requirements for the information system of third-party service providers, Estonian regulation lists the minimum requirements for the quality of information flow transmitting synchronized sound and image, requirements for recording and reproducibility of recording, and requirements for framing the face and document of a person. Regarding data retention, the Company must act under MLTFPA (2022, sec. 47 pp. 27-28). Therefore, the data and relevant documents that serve as the basis for establishing the business relationship, including documents collected for compliance purposes, as well as powers of attorney, must be collected and retained for five years after the end of the business relationship with the Client or after the completion of a transaction with the Client. The information that serves as the basis for the reporting obligation to the FIU must be retained for five years after the reporting obligation has been fulfilled.

Thus, it is possible to conclude that FATF standards and Estonian regulation by the Minister of Finance allow Company to hire third parties to perform CDD on its behalf, including verifying customer identities, beneficial owners, and the nature of business relationships. Third parties may also provide facilities for the retention of CDD records, while the regulatory responsibility for CDD rests with the Company, not the third party. Accordingly, the Company should ensure that the third party meets certain compliance criteria and is capable of doing so:

- meets the compliance standards outlined in FATF Recommendation 10 (2022b, 14-15) and Estonian regulation by the Minister of Finance (2018);
- provide copies of CDD data upon request of FIU and other regulators;
- complies with the record FATF's retention requirements and data retention requirements specified in MLTFPA (2022, sec. 24 p.16-17, sec. 47, p.27-28);
- meets the location-specific regulatory compliance standards.

3. ML/TF RISK MANAGEMENT FRAMEWORK OF REGISTRATION AGENT LEIPAPA OÜ

3.1. Risk assessment and Client ML/TF risk factors

The author has determined the Client ML/TF risk factors and prepared a risk assessment for the Company under MLTFPA (2022, sec. 13(1) p.8), taking into account the importance of its compliance with the Validation Agent status.

3.1.1. Country risk

Country risk is the risk that the Company will cooperate with countries whose economic, social, legal, and political conditions can contribute to the risk of ML and TF. Such conditions may also increase the risk that the Company will be involved in violation of international sanctions.

Countries and jurisdictions which have deficiencies in their national AML/CFT regime are considered high-risk subjects due to the lack of regulations preventing illicit activities. The Company is to use the list of the countries identified by credible sources (e.g., FATF). Considering country/geographical risk, the Company defines the following exposures:

1. Clients from countries that do not have adequate AML/CTF approaches;
2. Clients from countries listed as countries with a high level of corruption, according to the annual Transparency International Corruption Perception Index.
3. Clients registered and/or conducting business transactions with countries subject to sanctions, embargoes, or similar measures mentioned in the FATF List and the following sources:
    - The Office of Foreign Assets Control (OFAC) Sanctions, Sanctions Programs and Country Information, and other OFAC Sanctions Lists.
    - The United Nations Security Council's Sanctions List.
    - Her Majesty's (HM) Treasury List.
    - The EU Consolidated Sanctions List.
    - The EU Most Wanted Warnings.
    - The Bureau of Industry and Security.
    - The State Department Foreign Terrorist Organizations List and Non-Proliferation List.
    - US DOJ (FBI, DEA, US Marshals, and others).
    - Interpol's Most Wanted.
    - CBI List (The Central Bureau of Investigation).

4. Clients registered and/or conducting business transactions with countries that provide funding or support for terrorist activities have designated terrorist organizations operating within the country, as identified by the European Union or the United Nations, and/or insufficient measures in combating terrorism financing and terrorist activities;
5. Clients registered and/or have business transactions with jurisdictions defined as "tax heavens" and located outside the Company's target market region.

When deciding whether to enter into a relationship with a Politically Exposed Person (PEP) or their family members or close associates, geography plays an important role as well as the type of PEP and the type of business relationship. To have a balanced country risk assessment, at least the following factors should be considered in regards to PEPs, their family members, or close associates:

- the level of corruption in PEP's country;
- the stability of the government and the presence of ongoing conflicts;
- presence of reliable AML/CFT standards and practices in their country, showing confidence in the source of funds and assets.
- the level of transparency around the economy and tax practices in their country is on the level allowing to trust in how Company's services may be used.

Such an approach to defining country risk from the perspective of PEP ensures consistency in the application of due diligence measures for PEPs, their family members, or close associates, and helps with targeted ongoing monitoring. The author has also implemented a risk assessment methodology to determine the criteria for national cooperation taking into account the relevant guidelines of the European Banking Authority regarding risk factors.

At the moment of the research, the author determines the list of the countries specified in Appendix 10, that the Company must consider as unacceptable for starting any business relationship. The list was prepared following the Company's risk assessment, the internal policy of the Company, and the list of countries against which sanctions have been imposed by the European Union, the United Nations (UN), or the United States of America (under the information specified in the Sanctions Programs and Country Information (OFAC 2022)).

3.1.2. Ownership structure risk

Since a Legal Entity Identifier (LEI) itself has the main objective to verify owners who are behind the market participants ("who is who", "who owns whom" principles), the risk related to the ownership structure of the Client must be considered accordingly. The ownership

structure risk is the risk that the Company will cooperate with Clients who issue or are entitled to issue bearer shares (equity securities) or Clients whose ownership structure makes it difficult to identify the beneficial owner or obtain independent and reliable documentation proving the ownership and control structure. This risk also includes the risk that the beneficial owner of a Legal Entity is a PEP or sanctioned entity/person.

Based on the activity of the Company and the definition of LEI, all Clients of LEIpapa OÜ are Legal Entities, therefore, the risk arising from the Client's ownership structure will be high in the Company.

To mitigate the risk, the author has specified in the Company's internal rules and procedures the steps to be taken to determine the ultimate beneficiaries of the Clients. The extract from the document is presented in Appendix 11. It is also explained that the Company will not accept Clients, where it is not possible to identify the ultimate beneficial owners, including Clients (Legal Entities) issuing bearer shares.

In respect of the ultimate beneficial owners or representatives who are politically exposed persons (PEPs) or members of his or her family or close associates, the author determined further steps to mitigate the risk. This includes, among other measures, in-depth research in respect of the person's origin of funds and source of wealth.

The author points out that the following Clients shall be considered by the Company as having a higher risk of ML and TF:

1. Legal Entities that issue or are entitled to issue bearer shares (equities);
2. Legal Entities whose ownership or membership structure hampers the detection of the beneficial owner;
3. Legal Entities with beneficial owners or representatives who are politically exposed persons (PEPs) or members of his or her family or a close associates;
4. Societies, foundations, and legal arrangements equivalent to foundations that are not established for for-profit-gaining purposes;
5. External accountants, legal advisors or legal arrangements, and company service providers that act or open accounts with a financial institution on their behalf to perform financial operations on their client's behalf.

3.1.3. Business activity risk

Business activity risk is a risk that the Company will cooperate with Clients whose business or other activities present a high risk of ML/TF (based on the assessment of threats).

The author determined the following economic or other activities deemed as high risk:

- Gambling, gaming, or betting activities.
- Forex brokers, forex consulting, advisers.
- Trading in precious stones and metals.
- Art market participants.
- Intermediary services in real estate trading.
- Charities.
- Financial services, loans, and money lending businesses.
- The accountancy sector.
- Travel, booking, ticket agencies.
- Car dealers, boat dealers.
- Telecommunication services, computer network or information services, data storage, sharing services.
- Health and beauty product trading.
- Cash intensive businesses.
- Car washes, beauty salons, nail bars, etc.
- Crypto-related businesses.
- Consultancy services.
- Insurance companies and brokers.
- IT services that are not related to IT software or hardware manufacturing and trading.

The author points out that the Company must rate the high-risk activities specified above to decide whether a business relationship is acceptable. When the Company considers accepting the Clients engaged in the high-risk activities, the Company must take appropriate risk-mitigating measures. Among others, the author specified in the Company's procedure's measures of enhanced due diligence, which includes in-depth research, determining the number of documents to be received from the Client before the commencement of the business relationship and during the business relationship. It is also important to note, that the Company should not deal with persons behind the Clients, who are directly or indirectly involved in illegal or unregulated businesses, including, but not limited to:

- arms trade and defense;
- adult entertainment and pornography;
- synthetic stimulants;
- illegal drugs; illegal sale of prescription drugs;
- political or religious organizations;
- replicas;
- MLM (attracting new members basis).

3.1.4. Client type and Client relationship risks

Client type risk is a risk associated with the type of the Legal Entity. The author determines the most ML/TF risk presents Legal Entities that are the private companies, as no independent agencies are overviewing such companies and public disclosure obligations are minimal. The lowest ML/TF risk usually presents publicly listed companies that have information disclosure obligations and are audited. Other types of Clients considered with a high risk of ML/TF are special purpose vehicles, trusts, and funds, where the inherent risk of such companies is high due to their nature and purpose.

The Company is exposed to an ML/TF risk posed by Clients, where it has not established a record of transactional activity and general Client behavior. The risk is the highest for new Clients while it decreases as a long-term relationship with the Client is established, having a positive past track record of the Client's activity and transactions, information about the Client from reliable sources, general Client behavior that is in line with the Client information that is known to the Company. The following Clients shall be considered by the Company as having a higher risk of ML and TF by behavior type:

- Clients that live abroad in another jurisdiction, or using different jurisdictions without apparent economic or lawful purpose;
- Clients mentioned in the news and information sources for any type of negative knowledge or activity related to them (adverse media);
- lack of activity, not using the service of the Company regularly (i.e., missing LEI renewal date, Client's LEI has been lapsed for more than a year, etc.);
- transit operations when the account is debiting immediately after crediting;
- where there is no commercial rationale for the operations performed by the Client;
- requests for a complex transaction that has no apparent economic or lawful purpose.

The author has defined a list of indicators of the Client's suspicious activity. This risk is related to past Client behavior and transactional activity and the pre-defined indicators may trigger further investigation of the Client's activity. The number of automatic system-generated alerts based on those suspicious activity indicators as well as results from internal suspicious activity investigation may lead to an increased ML/TF risk as identified and assessed by the Company. In case The Company deems the ML/TF risk is unacceptable, it should consider terminating relationships with the Client based on the internal investigation with true positive results or where external suspicious activity reports (SARs) have been submitted.

3.1.5. Delivery channel risk

Client identification of Legal Entities and their beneficial owners is carried out remotely with no face-to-face contact with the Clients. The author has implemented the integration of a third-party technological solution provided by Sum and Substance Ltd (SumSub) for identity checks, sanction screening, and PEPs. As such the greatest risk to the Company is the remote Client identification, which makes it possible for individuals, using stolen data, to register LEI codes in the name of another person. Such risk is prevalently relevant for natural persons, acting as beneficial owners or attorneys of Legal Entities. In the event of remote identification, the responsible employee of the Company identifies the Client if relevant parts of the identity document and at least one additional supportive document which can be used to verify the identification data of the relevant natural person and the type and number of the identity card, country or issuing authority, date of issue and expiration date is provided by the Client.

However, the internal system of the Company is connected with the SumSub verification solution that uses iBeta compliant liveness technology based on AI. The neural network creates 3D FaceMaps to ensure that the live person is presented in front of the camera during the verification process. The system also ensures that users are physically present by creating a 3D FaceMap that is constantly referenced to authorize their future actions (transactions, logins, etc.). Such technology allows for to detection of spoofing attempts, reduces cases of multi-accounting, and ensures the true user initiates transactions, account deletion, LEI code transfer, or other key steps. Thus, the use of biometrics checks, backed up by AI algorithms, allows for the detection of popular and emerging attack vectors, presenting a reliable verification method performed under ISO/IEC 30107-3 (2017).

3.2. Integration with information technology solution provider

As stated before, the Company, as an AML obliged entity, is required by law to follow the KYC principle to prevent ML/TF, as well as to apply international restrictive measures such as international sanctions and prevent relevant violations. To start a business relationship Clients are asked for personal information, and the amount of information requested depends on the laws of each Client's jurisdiction.

Due to changing regulatory environments and the need to adapt quickly, the massive volume of manual work, that is unreliable and expensive to perform, the Board of the Company has

decided to integrate the Company's internal system with the solution provider that can assist in detecting individuals presenting higher risk and be complied with the regulations. Authentication through information technology can be considered an equivalent to verifying a Client representative identity face-to-face. In both cases, the KYC requirements must be met, and the person behind the Client must fill out a form and answer questions from the Company in the form of a direct conversation. When authenticating with an information technology means, the Company can run database queries at the same time as the authentication process and use the facial recognition feature. Provided the authentication process is recorded, the Company can review the process later if needed and can also present such data to FIU in case of suspicion to ML/TF. Authentication with an IT means, the quality of the information obtained, and the information system itself is subject to the requirements set out in a regulation issued by the Ministry of Finance of the Republic of Estonia (Minister of Finance, 2018). When innovative technological means are used to identify and verify the identity of the Client's representative, the Company shall evaluate the extent to which the solution increases the risks of ML/TF and, as a result, determine the level of risk for situations that do not involve direct contact. In doing so, the Company must take into account that an electronic verification method does not always per se entail a higher risk of ML/TF, especially if a system with a high level of reliability is used (Eesti Pangaliit, 2022b, 5).

According to SumSub (author's communication, 19 April 2022), their system is based on the basic requirements of AML/CFT regulations such as FATF, FINMA, FCA, CySEC, and MAS; the flow can be customized depending on Company's law and risk assessment. SumSub's Information Security Management System undergoes regular audits and is found to be compliant with standards ISO 27001, which is proven with the relevant certificate. Besides, SumSub has a Compliance Control Payment Card Industry Data Security Standard (PCI DSS) attestation of compliance as a service provider. The facial liveness detection system was successfully tested under ISO/IEC 30107-3 (2017). Policies, procedures, processes, and approaches established in SumSub concerning personal data processing are compliant with the requirements of the EU GDPR. The Client's data is encrypted and stored on GDPR-compliant Amazon servers, which are located in the European data centers classified as Tier III by the Uptime Institute, which meet TIA-942 and PCI DSS standards, under the GDPR and with the private law of the Company. The standard data retention period is five years, while the individual period may be determined based on the Company's legal requirements and/or risk assessment policy. Each applicant may access and customize their

personal data or make a reasoned written request to block the processing or transfer of data based on a particular situation. The documentation (SumSub, 2022b) also indicates that access to personal data processed in the system is strictly regulated. Each employee is granted a level of access that is objectively necessary for the performance of their official duties following the job plan. As part of its AML screening process, SumSub monitors global lists for fitness and probity, as well as global and national sanctions, including OFAC, UN, HMT, EU, DFAT, and many others from around the world in real-time using a customizable fuzzy matching algorithm that enables it to reduce the number of false positives while maintaining precision.

It is obvious from the information above that the SumSub system complies with all the requirements presented in the Republic of Estonia to providers serving for automatic verification of the Clients. According to Kert Võlly (author's interview, 6 December 2021), the Head of the supervision department at FIU, using the SumSub system is allowed, thus, the Board of the Company has decided to implement the integration of the SumSub system for the automatic verification process within the Company's workflow. Through the use of the information technology means, the Company is able to screen any Client regarding sanctions lists, criminal status, PEPs status, adverse media – all before establishing a relationship. The database of existing and active Clients is also regularly screened on an automated basis to monitor any changes in the status of individuals. A risk-based approach is applied technologically so that each individual is risk-assessed during onboarding, addressing all KYC/AML requirements.

Information technology provided by SumSub is used with internally developed logical rules and the internal IT system of the Company to create a robust and efficient system to automate the process and alert individuals with medium or high-risk profiles either in real-time or near real-time. During the first interaction, the Company uses SumSub's document and facial recognition technologies to ensure that all documents provided within the remoted identification process are genuine and not tampered with and that the person registering is identical to the one on the official document. A natural person or the legal representative of a Legal Entity confirms upon the establishment of a business relationship and the conclusion of a one-time transaction that:

1. they carry out the identification process personally;

2. the data submitted is true and complete, and they are aware of the consequences associated with the submission of incorrect, misleading, or incomplete information upon the establishment of a business relationship;
3. they meet the conditions stated by the Company for the establishment of business relationships and the conclusion of a one-time transaction;
4. they will show the personal data page of the valid ID document in front of the camera;
5. they acknowledge that the identification of a person and verification of a person's identity with information technology means take place according to the procedure set out in MLFTPA (2022, sec. 31 pp.19-20);
6. they acknowledge that identification and verification of their identity do not oblige LEIpapa OÜ to establish a business relationship or guarantee the accessibility of services;
7. they acknowledge that identification and verification of their identity with information technology means is considered unsuccessful if the identity verification provider rejects the uploaded ID.

Ongoing AML monitoring is the process that Company put in place to ensure that its business relationships are consistent. In this way, the Company keeps up-to-date the information about existing and actual Clients, especially the high-risk ones. Watchlists are databases of lists that the Company uses for regular identity checks of known or suspected terrorists, money launderers, fraudsters, sanctioned persons, or PEPs. Such sources include (SumSub, 2022a):

- The Office of Foreign Assets Control (OFAC) Sanctions.
- The United Nations Security Council's Sanctions List.
- Her Majesty's (HM) Treasury List.
- The EU Consolidated Sanctions List.
- The EU Most Wanted Warnings.
- The Bureau of Industry and Security.
- The State Department Foreign Terrorist Organizations List and Non-Proliferation List.
- US DOJ (FBI, DEA, US Marshals, and others).
- Interpol's Most Wanted.
- CBI List (The Central Bureau of Investigation).

Information on how ongoing AML checks and watchlist screening work is specified in the developed Internal rules and procedures of the Company (Appendix 11). In the next clause, the author proposes to consider the Client's risk rating with the use of a risk rating tool.

3.3. Client risk rating

Based on the risk assessment and the Client's risk factors, the author has developed and implemented an internal Client risk rating tool. This tool is used to evaluate the inherent

ML/TF risk of Clients and assign a risk category (of low, medium, high, or unacceptable risk) to each Client.

The calculation of the risk associated with each Client considers the relevant risk factors described in the previous paragraph and assigns a weight for each of the factors based on the importance perceived by the Company, which is based on the Company's risk profile.

E.g., product and delivery channel risk factors have a high impact on the overall risk rating of the Clients as stated in the Wolfsberg Group Guidance (2022, 6). In the case of the delivery channel, any fraudsters wish to remain anonymous and not to be later tied and convinced to money laundering, thus, the delivery channel has a high impact on the overall risk rating of the Clients as remote identification may significantly increase the risk of the Client remaining anonymous due to the use of stolen or otherwise compromised identity.

The author decided to use the following risk factors and weights for natural persons (beneficial owners or attorneys of Legal Entities) according to the risk assessment:

1. Country risk (based on the residency) – high impact.
2. Product and services risk (industry) – high impact.
3. Country risk (based on nationality) – medium impact.
4. Delivery channel – high impact.
5. The beneficial owner or representative is a politically exposed person (PEP) or a member of his or her family or a close associate – high impact.
6. Relationship and transactional activity (within ongoing CDD review) – medium impact.

The following risk factors and weights must be used for Legal Entities:

1. Country risk – a place of incorporation of the Client – high impact.
2. Country risk – nationality or residence (whichever has higher risk value) of the ultimate beneficial owner (UBO) – high impact.
3. Product and services risk – high impact.
4. Client business activities – medium impact.
5. Client relationship – low impact.
6. Client type – low impact;
7. Transactional activity (within ongoing CDD review) – medium impact.

The risk category assigned to the Client automatically by the risk rating tool may be manually overridden to high risk in case other specific high-risk factors are identified during the CDD procedure. The Company considers the following risk factors:

- Presence of a PEP, who has a direct connection with a Client or who is the Client's ultimate beneficial owner;

- Identification of severe negative news related to the Client or its beneficial owner;
- Ownership structure that includes 3 or more legal entities between the Client (Legal Entity) and the ultimate beneficial owner of the Client;
- Ownership structure including special purpose vehicle companies, trusts, funds, or similar legal arrangements obfuscating the true ownership and control structure of the Client.

The risk rating tool is implemented within the internal system of the Company, with customizable options (parameters) that can be modified according to the current risk appetite of the Company. For demonstration, the author has reflected the risk rating tool references (Appendix 12) and presented the sample output result of the risk rating tool for this thesis (Appendix 13).

CONCLUSION

ML and TF are major risks for financial institutions and other AML obliged entities, such as FinTechs, crypto, insurance, credit institutions, investment companies, trust and service providers, etc. ML/TF risks need to be known and minimized in the obliged entities. For this reason, global and local regulators have enacted strict AML laws for obliged entities, and failure to comply with these laws results in significant penalties and damage to reputation. Therefore, any obliged entity needs an effective ML/TF Risk Management Framework that increases its defense from crime and allows it to minimize its risk.

In the present study, the author has examined the structure of LEI Registration Agent LEIpapa OÜ headquartered in the Republic of Estonia, in regard to its compliance with the requirements of legislative acts and laws related to ML/TF. For this purpose, the author has defined a concept of ML/TF, analyzed legislative acts, guidelines, and recommendations related to ML/TF provided by FATF, Estonian FSA, and FIU, and defined competent authorities engaged in the prevention of ML/TF in the Republic of Estonia, summarized scientific and regulatory understandings of the ML risk management for the structure of Registration Agent. Besides, the risks related to ML/TF that the Registration Agent is facing when performing verification of Legal Entities were identified, assessed, and categorized. The brief characteristics of the Company and the processes taking place in the Company have been reviewed and linked with the previous study of the author, where the implementation of an automated verification system within the workflow of the Company has been analyzed, and the benefits of such interaction for the Company were proved. Taking into account considerations of the representative of the Estonian FIU, the author has determined legislative possibilities for verifying Clients using technical means provided by a third party and analyzed the capabilities of the SumSub verification system and its applicability for use within the workflow of the Registration Agent.

In the present study, the author has investigated the risk factors of the Registration Agent in the area of AML/CFT and identified the main problems in the existing risk assessment system, taking into account requirements specified in the MLTFPA and recommendations /reports from FATF. Based on the results obtained, the author has created a new risk assessment system for the Company and developed a risk rating tool, that is suitable to use

with the third-party service provider such as SumSub. The author has defined five components of the ML/TF Risk Management Framework:

1. risk identification;
2. risk measurement and risk assessment;
3. risk management;
4. risk reporting and monitoring;
5. risk governance.

The risk assessment system and the risk rating tool are the main components of the ML/TF Risk Management Framework, which should be approved by the certified experts in the field of ML/TF. The author decided to acquire a Delphi method, using an approbation of two experts from different countries (jurisdictions) that don't know each other, but both have an undeniable authority in the field of AML/CFT.

The first expert is an accredited financial investigator and detective, who was working within the London Asset Confiscation and Enforcement Unit and was responsible for a range of financial investigations including fraud and ML. The first expert currently provides services of professional financial advice and training to students from financial institutions and other areas on AML/CFT. The second expert is a representative of the Estonian FSA, who works in the AML department and is responsible for the implementation of AML/CFT guidelines and other measures for the obliged entities supervised by the Estonian FSA.

The author has developed the Internal rules and procedures for the Company in accordance with the current legislation. The document covers the rules governing the operations of the Company in the field of AML/CFT. The Framework is supported by an effective risk measurement and the limit system as well as risk data and systems. An adequate risk governance structure and competent staff are other key elements of the ML/TF Risk Management Framework.

Both experts have reviewed the risk assessment system created by the author within the present research and checked the developed risk rating tool for its compliance with the current laws and regulations, as well as applicability for use in the structure of the Validation Agent. After certain negotiations, positive feedback was received from both experts.

The possibility of using LEI data for AML checks is also approved and represented in the author's article published in the International Journal of Humanities and Natural Sciences,

and the article submitted for publishing in the Latvian journal of Administrative and Criminal Justice.

Overall, the ML/TF Risk Management Framework for LEIpapa OÜ has been developed, approved, and can be used both for the structure of the Registration Agent and within the structure of the Validation Agent. Thus, the aim of the study has been fully achieved. The results of the study can be used by any obliged entity acting as the LEI Registration Agent, or the LEI Validation Agent, in the Republic of Estonia.

REFERENCES

Association of Certified Anti-Money Laundering Specialists (ACAMS). (2019). *Study Guide CAMS Certification Exam* (Sixth Edition). https://www.aml101.com/CAMS_Study_Guide.pdf

Basel Committee on Banking Supervision (BCBS). (2020, July). *Sound management of risks related to money laundering and financing of terrorism*. Guidelines. https://www.bis.org/bcbs/publ/d505.pdf

Chen, J. (2021, April 17). *Know Your Client (KYC)*. https://www.investopedia.com/terms/k/knowyourclient.asp

Council of Europe. (1990). *Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime*. https://rm.coe.int/168007bd23

Council of Europe. (2005). *Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism*. https://rm.coe.int/168008371f

de Meijer, C., & treasuryXL. (2019, September 19). *Using Blockchain for Legal Entity Identifiers or LEIs*. https://treasuryxl.com/blog/using-blockchain-for-legal-entity-identifiers-or-leis/

Deloitte. (2015a). *CFO Insights. Compliance risks: What you don't contain can hurt you*. Publication. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-cfo-insights-compliance-risks-final.pdf

Deloitte. (2015b). *The changing role of compliance*. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/gx-financial-changing-role-compliance.pdf

Deloitte. (2021). *The State of Compliance Survey 2020*. https://www2.deloitte.com/content/dam/Deloitte/au/Documents/audit/22012021-state-of-Compliance-Survey-Publication-5.pdf

Eesti Pangaliit. (2022a). *Anti money laundering*. FAQ. https://www.pangaliit.ee/anti-money-laundering

Eesti Pangaliit. (2022b, February 22). *Anti money laundering, counter terrorism financing and enforcement of financial sanctions policy and guidelines*. Guidelines. https://www.pangaliit.ee/files/AML%20CTF%20guidlines%20EBA%2022.02.2022.pdf

ESMA. (2017, October 9). *Legal Entity Identifier (LEI)*. Briefing. https://www.esma.europa.eu/sites/default/files/library/esma70-145-238_lei_briefing_note.pdf

ESMA. (2018). *MIFID II*. https://www.esma.europa.eu/policy-rules/mifid-ii-and-mifir

ESRB. (2020). Recommendations of the European Systemic Risk Board (ESRB) on identifying legal entities. *Official Journal of the European Union*, *ESRB/2020/12*, 403/1-403/6. https://www.esrb.europa.eu/pub/pdf/recommendations/esrb.recommendation201126_on_identifying_legal_entities~89fd5f8f1e.en.pdf

Europe Human's Rights Watchdog. (2021). *Money Laundering*. https://www.europewatchdog.info/en/treaties_and_monitoring/money-laundering/

European Banking Authority (EBA). (2016). The European Banking Authority at a glance. *European Banking Authority*. https://doi.org/10.2853/571589

European Banking Authority (EBA). (2021a). *Final report on guidelines on 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 ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849*. https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/963637/Final%20Report%20on%20Guidelines%20on%20revised%20ML%20TF%20Risk%20Factors.pdf

European Banking Authority (EBA). (2021b). *Final report on guidelines on the characteristics of a risk-based approach to anti- money laundering and terrorist financing supervision, and the steps to be taken when conducting supervision on a risk-sensitive basis under Article 48(10) of Directive (EU) 2015/849 (amending the Joint Guidelines ESAs 2016 72).*

https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/EBA-GL-2021-16%20GL%20on%20RBA%20to%20AML%20CFT/1025507/EBA%20Final%20Report%20on%20GL%20on%20RBA%20AML%20CFT.pdf

European Council. (2022, April 4). *Different types of sanctions*. https://www.consilium.europa.eu/en/policies/sanctions/different-types/

European Parliament and the Council. (2018, June 19). *Directive (EU) 2018/843*. Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843&qid=1651425216415

FATF. (1989). *Financial Action Task Force on Money Laundering*. https://www.fatf-gafi.org/media/fatf/documents/reports/1990%20ENG.pdf

FATF. (2019). *Public Statement - October 2019*. Public Statement. https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/public-statement-october-2019.html

FATF. (2020). *Guidance on Digital Identity*. Guidance. https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf

FATF. (2021). *Who we are*. https://www.fatf-gafi.org/about/

FATF. (2022a). *Money Laundering FAQ*. https://www.fatf-gafi.org/faq/moneylaundering/

FATF. (2022b). The FATF Recommendations. In *Standard*. http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

FATF. (2022c). *What do we do*. https://www.fatf-gafi.org/about/whatwedo

FATF. (2022d). *Report on the State of Effectiveness Compliance with FATF Standards*. https://www.fatf-gafi.org/media/fatf/documents/recommendations/Report-on-the-State-of-Effectiveness-Compliance-with-FATF-Standards.pdf

Financial Supervision Authority Act. *Finantsinspektsiooni seadus* (*RT I 2001, 48, 267*. RT I 2001, 48, 267). https://www.riigiteataja.ee/en/eli/ee/515012020001/consolide/current

FinCEN. (2021). *History of Anti-Money Laundering Laws*. https://www.fincen.gov/history-anti-money-laundering-laws

FIU. (2021). *Overview of the activities of the Estonian Financial Intelligence Unit in 2020*. https://fiu.ee/en/media/130/download

FSA. (2018). *Advisory Guidelines of Finantsinspektsioon "Organisational solutions and preventive measures for credit and financial institutions to take against money laundering and terrorist financing"*. https://www.fi.ee/sites/default/files/2019-01/FI%20rahapesu%20t%C3%B5kestamise%20juhend%202018%20%28EN%29_pdf.pdf

FSA. (2021, November 18). *Prevention of money laundering in general*. https://fi.ee/en/finantsinspektsioon/prevention-money-laundering-general

FSB. (2012a). *A Global Legal Entity Identifier for Financial Markets*. https://www.fsb.org/wp-content/uploads/r_120608.pdf

FSB. (2012b). *G20 Leaders Declaration*. https://www.fsb.org/wp-content/uploads/g20_leaders_declaration_los_cabos_2012.pdf

FSB. (2019). *FSB publishes peer review of implementation of the Legal Entity Identifier* (Issue 15/2019, p. 1). FSB. https://www.fsb.org/wp-content/uploads/R280519-2.pdf

FSB. (2020, November 16). *About the FSB*. https://www.fsb.org/about/

GLEIF. (2018a). *Know Your Customer (KYC): The Challenges Faced by the Banking Sector When Onboarding New Client Organizations*. https://www.gleif.org/media/pages/lei-solutions/lei-in-kyc-a-new-future-for-legal-entity-identification/3c606c2205-1651241475/gleif-research-findings_challenges-onboarding-client-organizations-in-banking-sector_v1.0-final.pdf

GLEIF. (2018b). *Registration Agents*. https://www.gleif.org/en/about-lei/get-an-lei-find-lei-issuing-organizations/registration-agents

GLEIF. (2019). *GLEIF Registration Authorities List*. https://www.lei-worldwide.com/uploads/1/0/8/2/108222369/gleif_registration_authorities_list.pdf

GLEIF. (2020). *Master Agreement*. https://www.gleif.org/media/pages/about-lei/the-lifecycle-of-a-lei-issuer/gleif-accreditation-of-lei-issuers/required-documents/dc4c46e523-1651241474/2020-06-01-ma-master-agreement-1.3-final.pdf

GLEIF. (2021a). *About GLEIF*. https://www.gleif.org/en/about/this-is-gleif

GLEIF. (2021b). *About LEI. The Global LEI System*. https://www.gleif.org/en/about-lei/gleif-management-of-the-global-lei-system

GLEIF. (2021c). *Introducing the Legal Entity Identifier (LEI)*. https://www.gleif.org/en/about-lei/introducing-the-legal-entity-identifier-lei

GLEIF. (2021d). *LEI Data. Global LEI Index*. https://www.gleif.org/en/lei-data/global-lei-index/

GLEIF. (2021e). *LEI in KYC: A New Future for Legal Entity Identification*. https://www.gleif.org/en/lei-solutions/lei-in-kyc-a-new-future-for-legal-entity-identification

GLEIF. (2021f). *Level 1 Data: Who is Who*. https://www.gleif.org/en/lei-data/access-and-use-lei-data/level-1-data-who-is-who

GLEIF. (2021g). *Registration Agents*. https://www.gleif.org/en/about-lei/get-an-lei-find-lei-issuing-organizations/registration-agents

GLEIF. (2022a). *About LEI*. Get an LEI: Find LEI Issuing Organizations. https://www.gleif.org/en/about-lei/get-an-lei-find-lei-issuing-organizations

GLEIF. (2022b). *LEI Solutions*. https://www.gleif.org/en/lei-solutions/validation-agents

GLEIF. (2022c). *Managing LOU Dashboard by GLEIF*. Statistics. https://public.tableau.com/app/profile/gleif/viz/LOU_Dashboard/LEICount

GLEIF. (2020b). *Regulatory Oversight Committee (ROC)*. https://www.gleif.org/en/about/governance/regulatory-oversight-committee-roc

HM Revenue & Customs. (2021, August 4). *Risk assess your business for money laundering supervision*. Guidance. https://www.gov.uk/guidance/money-laundering-regulations-risk-assessments

HM Treasury. (2021). *National risk assessment of proliferation financing*. https://www.webarchive.org.uk/wayback/archive/20210923123232/https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1020000/National_risk_assessment_of_proliferation_financing.pdf

International Finance Corporation (IFC). (2019). *Anti-Money-Laundering (AML) & Countering Financing of Terrorism (CFT) Risk Management in Emerging Market Banks*. Good Practice Note. https://www.ifc.org/wps/wcm/connect/e7e10e94-3cd8-4f4c-b6f8-1e14ea9eff80/45464_IFC_AML_Report.pdf?MOD=AJPERES&CVID=mKKNshy

International Organization for Standardization (ISO). (2017). *Information technology — Biometric presentation attack detection — Part 3: Testing and reporting*. Standard. https://www.iso.org/standard/67381.html

International Organization for Standardization (ISO). (2018). *ISO 31000:2018(en) Risk management — Guidelines*. https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en

LEIregister. (2021). *What Is An LEI Number?* https://www.leinumber.com/what-is-lei-code/

Lovegrove, S. (2021, July 21). *Commission sets out proposed Directive as regards access of NCAs to centralised bank account registries through the single access point*. https://www.regulationtomorrow.com/eu/commission-sets-out-proposed-directive-as-regards-access-of-ncas-to-centralised-bank-account-registries-through-the-single-access-point

ManagedLEI. (2021). *The Importance of Legal Entity Identifiers (LEI)*. https://managedlei.com/the-importance-of-lei/

Minister of Finance. *Infotehnoloogiliste vahendite abil isikusamasuse tuvastamise ja andmete kontrollimise tehnilised nõuded ja kord*. (RT I, 25.05.2018, 17, Vastu võetud 23.05.2018 nr 25).

https://www.riigiteataja.ee/en/tolge/pdf/509012019003

Ministry of Finance. (2022, February 11). *Anti-Money Laundering*. https://www.fin.ee/en/financial-policy-and-external-relations/financial-and-entrepreneurship-policy/anti-money-laundering#fatf

Ministry of Foreign Affairs. (2021, October 29). *International Sanctions*. https://vm.ee/en/international-sanctions

MLTFPA. *Rahapesu ja terrorismi rahastamise tõkestamise seadus*. (RT I, 17.11.2017, 2). https://www.riigiteataja.ee/akt/112032022019

nibusinessinfo. (2021). *Risk management. Compliance and regulatory risk*. Guidelines. https://www.nibusinessinfo.co.uk/content/compliance-and-regulatory-risk

O'Dwyer, G. (2020, April 1). *Swedbank to rebuild anti-money laundering systems after damning report*. https://www.computerweekly.com/news/252480982/Swedbank-to-rebuild-anti-money-laundering-systems

One Hundred Seventh Congress of the United States of America. (2001). *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*. USA PATRIOT ACT. https://www.govinfo.gov/content/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf

Open Risk Manual. (2021). *Risk Framework*. https://www.openriskmanual.org/wiki/Risk_Framework

Posey, B. (2021a, October). *Risk Management Framework (RMF)*. https://www.techtarget.com/searchcio/definition/Risk-Management-Framework-RMF

Posey, B. (2021b, October). *Risk Reporting* https://searchcompliance.techtarget.com/definition/risk-reporting

President's Commission on Organized Crime of the United States. (1984). *Interim Report to the President and the Attorney General "THE CASH CONNECTION: Organized Crime, Financial Institutions, and Money Laundering."* https://www.ojp.gov/pdffiles1/Digitization/166517NCJRS.pdf

Rahvusvahelise sanktsiooni seadus (ISA). (RT I, 19.03.2019, 11, Redaktsiooni jõustumise kp: 15.03.2022) https://www.riigiteataja.ee/en/tolge/pdf/508032022003

Regulatory Oversight Committee (ROC). (2022). *The Regulatory Oversight Committee - ROC*. https://www.leiroc.org/

SumSub. (2022a). *How Watchlist Screening Works*. https://help.sumsub.com/products/how-watchlist-screening-works

SumSub. (2022b). *Sumsub Compliance and Data Protection Policy*. https://help.sumsub.com/faq/sumsub-compliance-and-data-protection-policy

The Wolfsberg Group. (2022). *Wolfsberg Group Guidance on Digital Customer Lifecycle Risk Management*. Guidance. https://www.wolfsberg-principles.com/sites/default/files/wb/Digital%20Customer%20Lifecycle%20Risk%20Management.pdf

Tiwari, M., Gepp, A., & Kumar, K. (2020). A review of money laundering literature: the state of research in key areas. *Pacific Accounting Review*, *32*(2), 271–303. https://doi.org/10.1108/PAR-06-2019-0065

Tucci, L. (2021, October). *What is risk management and why is it important?* https://searchcompliance.techtarget.com/definition/risk-management

Ubisecure OY. (2019). Legal Entity Reference Data (LE-RD): The Critical Need For Data Accuracy. *RapidLEI*. https://rapidlei.com/wp-content/uploads/2019/05/Legal-Entity-Reference-Data.pdf

United Nations Office on Drugs and Crime (UNODC). (1988). *United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*. 3. https://www.unodc.org/documents/commissions/CND/Int_Drug_Control_Conventions/Commentaries-OfficialRecords/1988Convention/1988_OFFICIAL_RECORDS_Volume_I_en.pdf

United Nations Office on Drugs and Crime (UNODC). (2003). *Money Laundering and the Financing of Terrorism: The United Nations Response*. Global Programme Against Money Laundering. https://www.imolin.org/pdf/imolin/UNres03e.pdf

United Nations Office on Drugs and Crime (UNODC). (2021). *Money Laundering*. https://www.unodc.org/unodc/en/money-laundering/overview.html

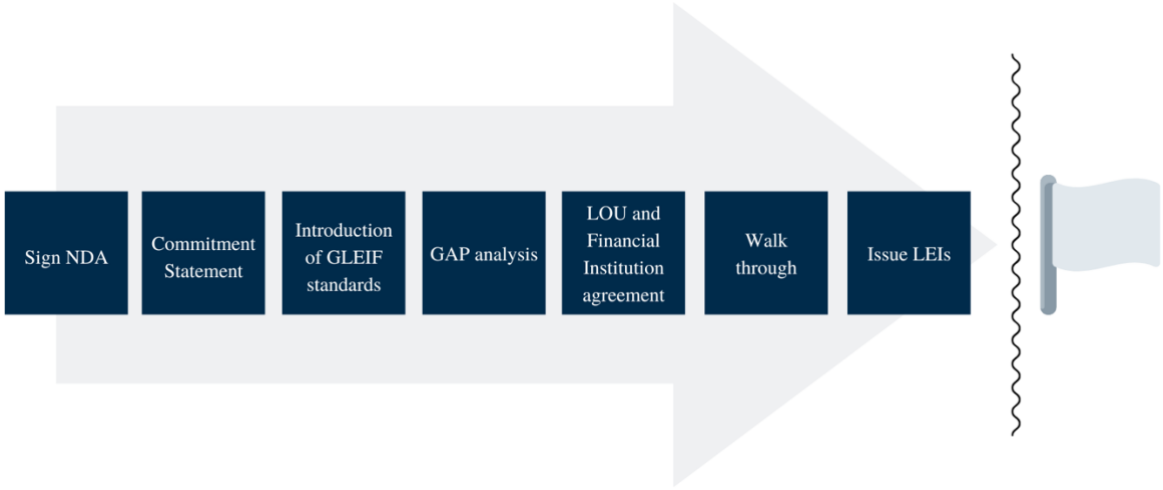
US Department of the Treasury, O. of F. A. C. (OFAC). (2022). *Sanctions Programs and Country Information*. https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information

Waite, S. (2020, May 28). *The new 'Conformity Flag' will enhance LEI trustworthiness and data quality*. https://rapidlei.com/lei-conformity-flag/

Jefremov, A., & Makhmudov, M. (2021). *Повышение эффективности действующих бизнес-процессов предприятия на примере LEIpapa OÜ*. Эстонский университет предпринимательства Майнор.

Кононова, Н., Патласов, О., & Кононов, Э. (2016). Риск-ориентированный подход в сфере противодействия отмыванию доходов и финансированию терроризма. *Наука о Человеке: Гуманитарные Исследования.*, *2*(24), 183–189. https://cyberleninka.ru/article/n/risk-orientirovannyy-podhod-v-sfere-protivodeystviya-otmyvaniyu-dohodov-i-finansirovaniyu-terrorizma/viewer

Appendix 1. GLEIS 2.0: Validation Agent Process Flow



Source: GLEIF, 2020

Appendix 2. The genesis of money laundering

Source	Definition
President's Commission on Organized Crime of the United States (1984)	"Money laundering" is the process by which one conceals the existence, illegal source, or illegal application of income, and then disguises that income to make it appear legitimate.
United Nations Office on Drugs and Crime (UNODC) (1988)	"Laundering" means the concealment or disguise of the true nature, source, disposition, movement, or ownership of proceeds and includes the movement or conversion of proceeds by electronic transmission.
FATF (1989)	Money laundering is the processing of these criminal proceeds to disguise their illegal origin.
Council of Europe (1990)	Laundering offenses – the conversion or transfer of property, knowing that such property proceeds, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of the predicate offense to evade the legal consequences of his actions.
USA PATRIOT ACT (2001)	ML – the movement of criminal proceeds and the financing of crime and terrorism.
ACAMS (2019)	Money laundering involves taking criminal proceeds and disguising their illegal sources to use the funds to perform legal or illegal activities.
(MLTFPA, 2022)	Money laundering' means the conversion or transfer of property derived from criminal activity or property obtained instead of such property for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's actions.

Source: (ACAMS, 2019; Council of Europe, 1990; FATF, 1989; MLTFPA, 2022; One Hundred Seventh Congress of the United States of America, 2001; President's Commission on Organized Crime of the United States, 1984; United Nations Office on Drugs and Crime (UNODC), 1988), edited by the author

Appendix 3. Possible tasks performed by a Registration Agent and the LEI issuing organization

According to (GLEIF, 2021g), the Registration Agent's role in the Global LEI System is directly connected to the LEI issuing organization. The Registration Agent may choose to partner with one or more LEI issuing organizations to ensure its clients' needs for LEI services are met.

Possible tasks performed by a Registration Agent include:

- Publish information on its website to help a legal entity apply for an LEI with an LEI issuing organization.
- Manage communications with the legal entity.
- Process or receive secure payment for the issuance or renewal of an LEI.
- Provide data collection or aggregation services from the relevant authoritative sources. (Reference data provided by the legal entity wishing to obtain an LEI is validated with a local authoritative source – a national Business Register, for example – before issuing an LEI compliant with the LEI standard.)
- Validate the legal entity reference data provided by a legal entity that wishes to obtain an LEI.
- Possible tasks performed by the LEI issuing organization include:
- Issue the LEI in compliance with ISO 17442:2012 standard along with the pertaining legal entity reference data (LE-RD).
- Upload to GLEIF the new LEI and all LE-RD.
- Review and respond to LEI or LE-RD challenges transmitted by GLEIF. (The centralized challenge facility made available by GLEIF extends the ability to trigger updates of LEI data to all interested parties).

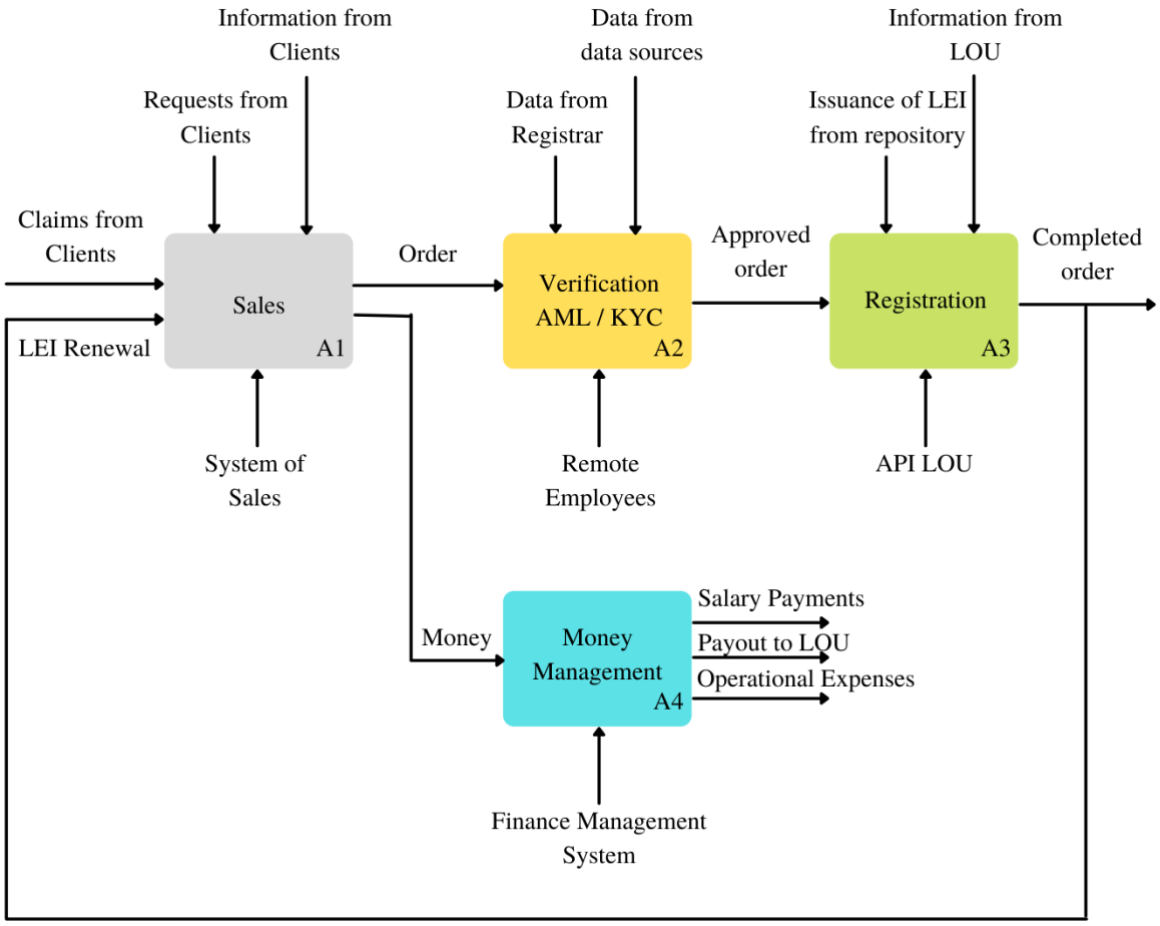
Registration Agents will neither be responsible for issuing LEIs nor will they have editorial access to LEI data.

Appendix 4. Services performed by Registration Agent according to Registration Agent agreement concluded with Managing LOU

According to the Registration Agent agreement concluded between LEIpapa OÜ, acting as a Registration Agent, and UBISECURE OY, acting as Managing LOU, services to be performed by the Registration Agent are as follows:

1. Publish information on its website to help a Legal Entity apply for an LEI with LOU.
2. Manage communications with the Legal Entity.
3. Manage or receive secure payment for the issuance or renewal of an LEI.
4. Provide data collection or aggregation services from the relevant authoritative sources.
   a) Reference Data provided by the Legal Entity wishing to obtain an LEI must be validated by a local authoritative source.
   b) LOU platform ordinarily will validate against the authoritative source but in certain cases, LOU may rely on the assistance of the Registration Agent to obtain the necessary information.
5. Validation of the legal Reference Data provided by a Legal Entity that wishes to obtain an LEI.
   a) LOU platform ordinarily will validate against the authoritative source but in certain cases, LOU may rely on the assistance of the Registration Agent to obtain the necessary information.
6. Obtain necessary authorization from each Legal Entity to act on its behalf.
   a) LOU will need to approve the terms and conditions of service provided by the Registration Agent to its Clients and capture such contract in the LOU management system if the signed letter of authorization is not obtained for all LEI registrations.
7. Obtain acceptance of the LOU terms of service for each LEI ordered.
   a) LOU will need to approve the terms and conditions of service provided by the Registration Agent to its Clients and capture such contract in the LOU management system if the LOU terms of services are not individually e-signed per LEI registration.
   b) The Registration Agent agrees to be bound by the terms of service which govern the use of the LOU management system by using any or all the services.

Appendix 5. IDEF0 methodology diagram of LEIpapa OÜ business processes



Source: (Jefremov & Makhmudov, 2021, 35)

Appendix 6. Document requirements for LEI applications

DOCUMENT REQUIREMENTS FOR LEI APPLICATIONS

This guide covers what documents need to be submitted for a successful LEI application with RapidLEI.

DEFINING THE ENTITY TYPE

There are several different entity types that are eligible for LEI applications.

- **Legal Entity -** a Registered legal entity is any company or organization that has legal rights and responsibilities
- **Trust**: a Trust is a structure where a trustee carries out the business on behalf of the trust's members (or beneficiaries)
- **Fund**: a Fund is an investment vehicle with money raised to invest
- **Will/Pension**: a legally enforceable declaration of how a person wants their property and assets distributed after death
- **Other**: in the RapidLEI Shopping Cart, under the Entity Type selection box, you will see "other" this is for Partners who aren't sure what Entity Type it is that they are applying for.

LEVEL 1 & LEVEL 2 APPLICATIONS

LEVEL 1 LEI DESCRIPTION

When published, LEI codes are delivered with an underlying Common Data Format (CDF) structure. This Legal Entity Reference Data (LE-RD) covers items such as Legal Entity Form, Legal Entity Status, Legal Name and Legal Entity Address. The Global LEI Foundation (GLEIF) refers to this as Level 1 data. i.e. Who is Who.

LEVEL 1 NEW APPLICATIONS

The RapidLEI Vetting Team will require the following documentation to process new orders submitted for;

Legal Entity:

- RapidLEI Partner T&C's or a Letter of Authorisation (LoA)

Trust:

- RapidLEI Partner T&C's or a Letter of Authorisation (LoA) and a copy of the Trust Deed.

Fund:

- RapidLEI Partner T&C's or a Letter of Authorisation (LoA) and a copy of the funds statutory prospectus or fact sheet

Will/Pension

- RapidLEI Partner T&C's or a Letter of Authorisation (LoA) and a copy of the pension plan / Will Testament

Other

- RapidLEI Partner T&C's or a Letter of Authorisation (LoA)

LEVEL 1 IMPORT APPLICATIONS

When importing an LEI from another LOU, a Letter of Authorisation (LoA) is mandatory. The LoA will be shared between LOUs to meet the transfer requirements. Other LOU's do not accept RapidLEI T&C's alone.

The other requirements stated above in relation to entity type also apply.

LEVEL 1 SUPPORTING DOCUMENTATION

The following documents may be required by our Vetting Team to support certain applications where the data is not available to them via the GLEIF Registration Authoirties;

- Articles of Incorporation (US, Canada)
- Articles of Association
- Certificate of Incumbency
- Resolution of Directors
- Memorandum of Association
- Meeting Minutes (Signed, Headed document)
- If the applicant is listed under the company website as an employee/director.
- Deed (Applicable for Trusts/Funds/Wills/Pensions)

If you are unable to obtain these relevant documents please let us know via support@rapidlei.com and we will work with you to find an altenative source suitable for us to be able to make the appropriate validation checks for your application.

For questions or further information contact your Account Manager or support@rapidlei.com. Version Q1.1 2021

LEVEL 2 LEI DESCRIPTION

Level 2 data was introduced in May 2017 to provide details of Who owns Whom. Where parents exist (parent being defined from an accounts consolidation perspective) then Legal Entity Relationship Records (LE-RR)s are also delivered in a CDF structure. If no Ultimate or Direct parents exist then Exception Records are necessary. Ideally LE-RR data delivers the LEI codes of parents as part of the data structure, however, in cases where an LEI has not yet been issued to a parent then PRD (Parent Reference Data) is taken to help the GLEIF build a better picture of relationships to ensure enhancements to the Global LEI System (GLEIS) model are effective.

Further information is provided in the RapidLEI FAQ pages: https://rapidlei.com/faq/lei-application-process/

LEVEL 2 APPLICATIONS & SUPPORTING DOCUMENTATION

Level 2 applications predominantly apply to Legal Entities but it may also apply to Funds/Trusts. RapidLEI can provide a Level 2 Data Validation document to assist with level 2 orders.

Level 2 applications for Legal Entities can supply:

- Consolidated Financial Statements
- Regulatory Fillings
- Financial Statements

Notes on understanding of how Parental Structures work:

- An entity is only classed as a parent if they own/consolidate 50% or more of the child/direct parent.
- If there are two parents with equal ownership - 50/50, then the GLEIF's definition of this is that the child does not have a parent.
- Consolidated accounts per parent are only required if the direct and ultimate parent are not the same legal entity.
- Applications should contain the most up to date consolidated accounts, however, we will accept up to 2 years old.
- Consolidated accounts are the preferred supporting documentation for validation as these can fully corroborate the parental relationship.

Source: Internal documents of the Managing LOU

Appendix 7. Rules of Procedure for Monitoring Money Laundering and Terrorist Financing and Compliance with International Sanctions

RULES OF PROCEDURE
FOR PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING
AND
COMPLIANCE WITH INTERNATIONAL SANCTIONS

Established by the decision of the management board of LEIpapa OÜ, registry code 16283000, on 02.08.2021

1. General provisions

1.1. These rules of procedure for prevention of money laundering and terrorist financing, and compliance with international sanctions (hereinafter **Rules**) lay down requirements for screening the Clients (as defined in section 2.7) in order to prevent entering into deals involving suspected Money Laundering and Terrorist Financing, and to ensure identification and reporting of such.

1.2. The obligation to observe the Rules rests with Management Board members and employees of the Provider of service, including temporary staff, agents of the Provider of service who initiate or establish Business Relationship (as defined in section 2.6) (hereinafter all together called the **Representative**). Every Representative must confirm awareness of the Rules with the signature.

1.3. The Rules are primarily based on the regulations of Money Laundering and Terrorist Financing Prevention Act (hereinafter **the Act**) and International Sanctions Act (hereinafter **ISA**).

1.4. All relevant employees should know and strictly follow the requirements set out in the Money Laundering and Terrorist Financing Prevention Act, the guidelines on the characteristics of suspicious transactions possibly involving money laundering and terrorist financing, other guidelines on compliance with the Act pertaining to the activities of the company as well as these Rules of Procedure.

1.5. All relevant employees should keep themselves up to date with any amendments to the legislation and with other legal acts published on the website of the Financial Intelligence Unit (hereinafter **FIU**) at: https://www.fiu.ee/en and guidelines of Financial Supervisory Authority (hereinafter **FSA**) at: https://www.fi.ee/en/guides/pangandus-ja-krediit/organisational-solutions-and-preventive-measures-credit-and-financial-institutions-take-against

1.6. A copy of these Rules of Procedure shall be available to all relevant employees.

2. Definitions

2.1. Money Laundering – is a set of activities with the property derived from criminal activity or property obtained instead of such property with the purpose to:

i. conceal or disguise the true nature, source, location, disposition, movement, right of ownership or other rights related to such property;

ii. convert, transfer, acquire, possess or use such property for the purpose of concealing or disguising the illicit origin of property or of assisting a person who is involved in criminal activity to evade the legal consequences of his or her action;

iii. participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to subsections 2.1.i and 2.1.ii.

2.2. Terrorist Financing – acts of financing of terrorism as defined in § 237^3 of the Penal Code of Estonia.

2.3. International Sanctions – list of non-military measures decided by the European Union, the United Nations, another international organisation or the government of the Republic of Estonia and aimed to maintain or restore peace, prevent conflicts and restore international security, support and reinforce democracy, follow the rule of law, human rights and international law and achieve other objectives of the common foreign and security policy of the European Union.

2.4. Compliance Officer or CO – representative appointed by the Management Board responsible for the effectiveness of the Rules, conducting compliance over the adherence to the Rules and serving as contact person of the FIU.

2.5. FIU - Financial Intelligence Unit of the Police and Border Guard Board of Estonia.

2.6. Business Relationship – a relationship of the Provider of service established in its economic and professional activities with the Client.

2.7. Client – a natural or legal person, who uses services of the Provider of service.

2.8. Beneficial Owner – is a natural person, who:

i. Taking advantage of his influence, exercises control over a transaction, operation or another person and in whose interests or favour or on whose account a transaction or operation is performed taking advantage of his influence, makes a transaction, act, action, operation or step or otherwise exercises control over a transaction, act, action, operation or step or over another person and in whose interests or favour or on whose account a transaction or act, action, operation or step is made.

ii. Ultimately owns or controls a legal person through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that person, including through bearer shareholdings, or through control via other means. Direct ownership is a manner of exercising control whereby a natural person holds a shareholding of 25 per cent plus one share or an ownership interest of more than 25 per cent in a company. Indirect ownership is a manner of exercising control whereby a company which is under the control of a natural person holds or multiple companies which are under the control of the same natural person hold a shareholding of 25 per cent plus one share or an ownership interest of more than 25 per cent in a company.

iii. Holds the position of a senior managing official, if, after all possible means of identification have been exhausted, the person specified in clause ii cannot be identified and there is no doubt that such person exists or where there are doubts as to whether the identified person is a beneficial owner.

iv. In the case of a trust, civil law partnership, community or legal arrangement, the beneficial owner is the natural person who ultimately controls the association via direct or indirect ownership or otherwise and is such associations': settlor or person who has handed over property to the asset pool, trustee or manager or possessor of the property, person ensuring and controlling the preservation of property, where such person has been appointed, or the beneficiary, or where the beneficiary or beneficiaries have yet to be determined, the class of persons in whose main interest such association is set up or operates.

2.9. Politically Exposed Person or PEP - is a natural person who is or who has been entrusted with prominent public functions including a head of state, head of government, minister and deputy or assistant minister; a member of parliament or of a similar legislative body, a member of a governing body of a political party, a member of a supreme court, a member of a court of auditors or of the board of a central bank; an ambassador, a chargé d'affaires and a high-ranking officer in the armed forces; a member of an administrative, management or supervisory body of a state-owned enterprise; a director, deputy director and member of the board or equivalent function of an international organisation, except middle-ranking or more junior officials.

2.9.1. The provisions set out above also include positions in the European Union and in other international organizations.

2.9.2. A family member of a person performing prominent public functions is the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person; a child and their spouse, or a person considered to be equivalent to a spouse, of a politically exposed person; a parent of a politically exposed person.

2.9.3. A close associate of a person performing prominent public functions is a natural person who is known to be the beneficial owner or to have joint beneficial ownership of a legal person or a legal arrangement, or any other close business relations, with a politically exposed person; and a natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person.

2.10. Local Politically Exposed Person or local PEP – a natural person, provided in section 2.9, who performs or has performed prominent public functions in Estonia, a contracting state of the European Economic Area or in an institution of European Union.

2.11. Provider of service – LEIpapa OÜ

2.12. Management Board or MB – management board of the Provider of service. Members of the MB, as appointed by relevant MB decision, are responsible for implementation of the Rules.

3. Description of activities of the Provider of service

3.1. The Provider of service is the LEI Registration Agent.

3.2. The Provider of service is a subject to authorisation by the FIU.

4. Compliance Officer

4.1. The MB shall appoint a CO whose principal tasks are to:

4.1.1. monitor the compliance of the Rules with the relevant laws and compliance of the activity of the Representatives with the procedures established by the Rules;

4.1.2. compile and keep updated the data regarding countries with low tax risk, high and low risk of Money Laundering and Terrorist Financing and economical activities with great exposure to Money Laundering and Terrorist Financing;
4.1.3. carry out training, instruct and update the Representatives on matters pertaining to procedures for prevention of Money Laundering and Terrorist Financing;
4.1.4. report to the MB once a year (or more frequently, if necessary) on compliance with the Rules, and on circumstances with a suspicion of Money Laundering or Terrorist Financing;
4.1.5. collect, process and analyse the data received from the Representatives or Clients concerning suspicious and unusual activities;
4.1.6. collaborate with and report to the FIU on events of suspected Money Laundering or Terrorist Financing, and respond to enquiries of the FIU;
4.1.7. make proposals on remedying any deficiencies identified in the course of checks.

4.2. The CO must meet all the requirements, prescribed by the Act, and appointment of the CO shall be coordinated with the FIU. If, as a result of a background check carried out by the FIU, it becomes evident that the CO's credibility is under suspicion due to their previous acts or omissions, the Provider of service may extraordinarily terminate the CO's employment contract due to the loss of credibility.

4.3. Tasks of the CO can be performed by a department, therefore provisions of section 4.2 will apply accordingly.

5. Application of due diligence measures

5.1. The Provider of service shall determine and take due diligence (hereinafter **DD**) measures using results of conducted risk assessment (see Section 10), and provisions of national risk assessment, published on the web-page of the Ministry of Finance of Estonia.

5.2. The Representatives shall pay special attention to circumstances that refer to Money Laundering or Terrorist Financing.

5.3. Depending on the level of the risk of the Client and depending on the fact whether the Business Relationship is an existing one or it is about to be established, the Provider of service shall apply either normal DD measures (see Section 6), simplified DD measures (see Section 8) or enhanced DD measures (see Section 9). The Provider of service shall also apply continuous DD measures to ensure ongoing monitoring of Business Relationships (see Sections 5.7-5.10). The objective of applying the DD measures is, among others, to identify complicated, high-value and unusual transactions and transaction patterns that do not have any reasonable or obvious economic or legitimate purpose or are uncharacteristic of the specific features of the business in question.

5.4. DD measures shall include the following procedures:

- **i.** Identifying the Client and verifying its identity using reliable, independent sources, documents or data, including e-identifying;
- **ii.** Identifying and verifying of the representative of the Client and the right of representation;
- **iii.** Identifying the Client's Beneficial Owner;
- **iv.** Assessing and, as appropriate, obtaining information on the purpose of the Business Relationship;
- **v.** Conducting ongoing DD on the Client's business to ensure the Provider of service's knowledge of the Client and its source of funds is correct;
- **vi.** Obtaining information whether the Client is a PEP or PEP's family member or PEP's close associate.

5.5. In the case of transactions the obliged entity must consider the customer's risk
profile and associated risks and the risk assessment of the obliged entity, in the relevant case identify

5.6. The Provider of service shall establish the source of wealth of the Client, where appropriate.

5.7. To comply with the DD obligation, the Representatives shall have the right and obligation to:
- **i.** request appropriate identity documents to identify the Client and its representatives;
- **ii.** request documents and information regarding the activities of the Client and legal origin of funds;
- **iii.** request information about Beneficial Owners of a legal person;
- **iv.** screen the risk profile of the Client, select the appropriate DD measures, assess the risk whether the Client is or may become involved in Money Laundering or Terrorist Financing;
- **v.** re-identify the Client or the representative of the Client, if there are any doubts regarding the correctness of the information received in the course of initial identification;

5.8. The objective of the continuously applied DD measures is to ensure on-going monitoring of Clients. Conducting ongoing monitoring of the Business Relationship includes:
- i. Keeping up-to-date the documents, data or information, obtained during taking DD measures;
- ii. Paying particular attention Client's conduction, leading to criminal activity or Money Laundering or Terrorist Financing;
- iii. Paying particular attention to the Business Relationship, if the Client is from or the seat of a Client being a legal person is located in a third country, which is included in the list of risk countries (see Exhibit 1).

5.9. Annual review of a Client being a legal entity is carried out regularly once a year. Updated data shall be recorded in the Provider of service's Client database and added to LEI Reference Data.

5.10. The Representative updates the data of a Client, who is either a legal person or a natural person, i.e. takes appropriate DD measures every time when:

i. the Client addresses the Provider of service with the request to amend a long-term contract during the term of its validity;

ii. Upon identification and verification of the information there is reason to suspect that the documents or data gathered earlier are insufficient, have changed or are incorrect. In this case, the Representative may conduct a face-to-face meeting with the Client;

iii. the Provider of service has learned through third persons or the media that the activities or data of the Client have changed significantly.

5.11. The Representative shall evaluate the substance and the purpose of the Client's activities, in order to establish the possible links with Money Laundering or Terrorist Financing. The evaluation should result in an understanding about the purpose of the Business Relationship for the Client, the nature of the Client's business, the risk levels of the Client and, if necessary, the sources of funds.

6. Normal due diligence measures

6.1. The Provider of service shall conduct normal DD in the following cases:
- **i.** Upon establishing a new Business Relationship;
- **ii.** In the event of insufficiency or suspected incorrectness of the documents or information gathered previously in the course of carrying out DD measures;

6.2. In the course of conducting normal DD measures, the Representative shall apply the measures of DD as provided for in section 5.4.

6.3. No new Business Relationship can be formed, if the Client, in spite of the respective request, has failed to present documents and appropriate information required to conduct DD, or if based on the presented documents, the Representative suspects Money Laundering or Terrorist Financing.

6.4. If in spite of the respective request an existing Client has failed to present during the contract period documents and appropriate information required to conduct DD, such behaviour constitutes material breach of contract that shall be reported by the Representative to the CO, and in such case the contract(s) concluded with the Client shall be cancelled and the Business Relationship shall be terminated as soon as feasible[1].

6.5. The Provider of service shall not enter into Business Relationships with anonymous Clients.

[1] The termination of the long-term contract or contract without the term must foresee the Provider of service's right to terminate the contract extraordinarily without observing the period of pre-notice in case the Client does not provide requested identification or verification documents (in due time)

7. Identification of a person

7.1. Upon implementing DD measures the following person shall be identified:

i. Client – a legal person;
ii. Representative of the Client – an individual who is authorized to act on behalf of the Client;
iii. Beneficial Owner of the Client;
iv. PEP – if the PEP is the Client or a person connected with the Client (see Section 2.9).

7.2. **Upon establishing the relationship with the Client, the Provider of service shall identify and verify the Client while being present at the same place as the Client or by using information technology means.**

7.3. For identification of a Client and verification of the identity of a Client by using information technology means, the Provider of service shall use:

7.3.1. a document issued by the Republic of Estonia for the purpose of digital identification;

7.3.2. another electronic identification system within the meaning of the Regulation (EU) No 910/2014 of the European Parliament and of the Council[2]. If the Client is a foreign national, the identity document issued by the competent authority of the foreign country is also used simultaneously.

7.4. In case of identification of a Client and verification of the identity of a Client by using information technology means the Provider of service shall additionally obtain data from a reliable and independent source, e.g. identity documents databases.

7.5. Identification of a representative of a Client

7.5.1. Upon establishing a Business Relationship, identification takes place, above all, during a face-to-face meeting or by using information technology means.

7.5.2. The Rules must be considered when dealing with the documents that can be used to identify the Client or its representative and the requirements established for them (see Section 7.10). If it is not possible to obtain original documents for identification of a Client, request documents certified or authenticated by a notary public or authenticated officially for verification of the identity of the natural person, or use data obtained from other reliable and independent sources (including electronic identification) on condition that information is obtained from at least two different sources.

7.5.3. Verification must be made whether or not such a person is a PEP (see Section 7.9).

7.5.4. A new Client and, if necessary, an existing Client shall confirm the correctness of the submitted information and data by signing the Client data registration sheet (see Form 1).

7.6. Identification of a Client

7.6.1. To identify a Client who is a legal person, the Representative shall take the following actions:

i. Check the information concerning a legal person by accessing the relevant electronic databases (e-commercial register/ e-äriregister and European Business Register);

ii. If it is not possible to obtain an original extract from the register or the respective data, request documents (extract from the relevant registry, certificate of registration or equivalent document) certified or authenticated by a notary public or authenticated officially for verification of the identity of the legal person, or use data obtained from other reliable and independent sources (including electronic identification) on condition that information is obtained from at least two different sources;

iii. Ask the representative of a foreign legal person to present an identity documents and a document evidencing of his/her power of attorney, which has been notarised or authenticated pursuant to an equal procedure and legalised or authenticated by a certificate substituting for legalisation (apostille), unless otherwise prescribed by an international agreement;

iv. On the basis of the information received from the representative of the foreign legal person, control whether or not the legal person could be linked with a PEP (see Section 7.9);

[2] http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1510127223064&uri=CELEX:32014R0910

v. If the seat of a Client being a legal person is located in a third country, which is included in the list of risk countries (see Exhibit 1), report this to the CO, who shall decide the additional measures to be applied to identifying and background checking of the person.

7.6.2. The document presented for identification of a legal person shall set out at least the following:

i. business name, registry code (number), date of registration, seat and address;

ii. names and authorisations of members of the Management Board or the head of branch or the other relevant body.

7.6.3. A legal representative of a new Client (subsequently as required) shall confirm the correctness of the submitted information and data by signing the Client data registration sheet (see Form 1).

7.7. Consequences of insufficient identification of a Client

7.7.1. Should the Representative establish that the identification of a Client is insufficient the Representative shall:

i. Promptly apply the enhanced DD measures pursuant to the Rules;

ii. Notify the CO of the failure to implement normal DD in a timely manner;

iii. Assess the risk profile of the Client and notify CO and/or MB for the purposes of the provisions in Section 12.3.

7.8. Identification of the Beneficial Owner of the Client

7.8.1. Registration and assessment of the Beneficial Owner(s) of a legal person is mandatory.

7.8.2. There is no need to identify the Beneficial Owners of a Client/company whose securities have been accepted for trading on a regulated securities market.

7.8.3. In order to establish the Beneficial Owner, the Representative shall take the following actions:

i. Gather information about the ownership and control structure of the Client on the basis of information provided in pre-contractual negotiations or obtained from another reliable and independent source;

ii. In situations, where no single person holds the interest or ascertained level of control to the extent of no less than 25 per cent (see Section 2.9), apply the principle of proportionality to establishing the circle of beneficiaries, which means asking information about persons, who control the operations of the legal person, or otherwise exercise dominant influence over the same;

iii. If the documents used to identify a legal person, or other submitted documents do not clearly identify the Beneficial Owners, record the respective information (i.e. whether the legal person is a part of a group, and the identifiable ownership and management structure of the group) on the basis of the statements made by the representative of the legal person, or a written document under the hand of the representative;

iv. To verify the presented information, make enquiries to the respective registers, and request an annual report or another appropriate document to be presented.

v. If no natural person is identifiable who ultimately owns or exerts control over a Client and all other means of identification are exhausted, the senior managing official(s) might be considered to be the Beneficial Owner(s).

vi. Pay attention to companies established in low tax rate regions (see Exhibit 1).

7.8.4. While establishing the Beneficial Owner, it is possible to rely on information received in a format reproducible in writing from a credit institution registered in the Estonian commercial register or from the branch of a foreign credit institution, or from a credit institution that has been registered or whose place of business is in a contracting state of the European Economic Area.

7.9. Identification of Politically Exposed Person

7.9.1. The Representative shall implement the following measures to establish whether or not a person is a PEP:

i. asking the Client to provide necessary information;

ii. making an enquiry or checking the data on websites of the respective supervisory authorities or institutions of the country of location of the Client;

iii. making an inquiry to the special PEP databases.

7.9.2. The matter of whether to establish a Business Relationship with a PEP, or a person associated with him or her, and the DD measures applied to such person shall be decided by the MB.

7.9.3. If a Business Relationship has been established with a Client, and the Client or its Beneficial Owner subsequently turns out to be or becomes a PEP, CO and MB shall be notified of that.

7.9.4. In order to establish a Business Relationship with a PEP or a company connected with that person, it is necessary to:

- **i.** take enhanced DD measures (see Section 9);
- **ii.** establish the source of wealth of this person;
- **iii.** monitor the Business Relationship on a continual basis at least once per 6 months.

7.9.5. DD measures, mentioned in Section 7.9.4 might be not applicable regarding local PEPs, if there are no relevant circumstances, leading to the higher risks.

7.9.6. Respective remarks must be made in the Provider of service's database of Clients on documents of such a person in the form of notation "Politically Exposed Person".

7.10. Documents that can be used for identification

7.10.1. In case of the representatives of Clients, the following documents can be used for identification[3]:

- **i.** Personal ID card (whether ID card, e-resident card or residence permit card);
- **ii.** Passport or diplomatic passport;
- **iii.** Travel document issued in a foreign country;
- **iv.** Driving licence (if it has name, facial image, signature and personal code or date of birth of holder on it).

7.10.2. The Representative shall make a copy of the page of the identity document which contains personal data and photo.

7.10.3. In addition to an identity document, the representative of a Client shall submit a document in the required format certifying the right of representation.

7.10.4. Legal person and its passive legal capacity shall be identified and verified on the basis of the following documents:

- **i.** in case of legal persons registered in Estonia and branches of foreign companies registered in Estonia, the identification shall be conducted on the basis of an extract of a registry card of commercial register;
- ii. foreign legal persons shall be identified on the basis of an extract of the relevant register or a transcript of the registration certificate or an equal document, which has been issued by competent authority or body not earlier than six months before submission thereof.

7.10.5. If not original documents are used for identification, the Representative shall control and verify data by using at least two reliable and independent sources.

8. Simplified due diligence measures

8.1. Simplified DD measures may be taken, if the Client is:

- i. A company listed on a regulated market that is subject to disclosure requirements consistent with European Union law;
- ii. a legal person governed by public law founded in Estonia;
- iii. an authority of the European Union;
- iv. a credit institution or a financial institution, acting on behalf of itself, located in a contracting state of the European Economic Area or in a third country (see Exhibit 1), which in the country of location is subject to equal requirements and the performance of which is subject to state supervision.

9. Enhanced due diligence measures

9.1. Enhanced DD measures must be taken in cases where the risk level of the Client is higher.

---

[3] About documents to be used for identification: https://www.politsei.ee/et/organisatsioon/rahapesu/kasulikku/isikusamasuse-tuvastamine.dot
Authenticity of personal ID documents can be checked here: http://www.consilium.europa.eu/prado/ET/prado-start-page.html (14.02.2017) or here: https://www.politsei.ee/et/teenused/e-paringud/dokumendi-kehtivuse-kontroll/

9.2. The Representative shall establish the Client's risk profile and determine the risk category in accordance with the Rules (see Section 10). The risk category may be altered during the course of the Business Relationship, taking into consideration the changes in data gathered.

9.3. The Representative, who upon entering into a Business Relationship with a new Client, detects that there is at least one of the following high-risk characteristics present in respect of a Client, shall consult with and report to the CO, and shall take the DD measures set out in the Rules.

9.4. The Representative shall apply enhanced DD measures in the following situations:

9.4.1. when suspicion arises regarding truthfulness of the provided data and/or of authenticity of the identification documents regarding the Client or its Beneficial Owners;

9.4.2. the Client is a PEP (excluding local PEPs, if there are no relevant circumstances, leading to the higher risks);

9.4.3. the Client is from or the seat of a Client being a legal person is located in a third country, which is included in the list of risk countries (see Exhibit 1);

9.4.4. in case of companies that have nominee shareholders or shares in bearer form;

9.4.5. in a situation with higher risk of Money Laundering and terrorists financing as described in Sections 9.1 and 9.3.

9.5. Enhanced DD measures shall include at least one the following measures in addition to normal DD measures as established in Section 5.4:

9.5.1. Identification and verification of a Client on the basis of additional documents, data or information, which originates from a reliable and independent source;

9.5.2. Identification and verification of a Client while being present at the same place;

9.5.3. Asking the identification or verification documents to be notarised or officially authenticated;

9.5.4. Obtaining additional information on the purpose and nature of the Business Relationship and verification from a reliable and independent source;

9.5.5. the making of the first payment related to a transaction via an account that has been opened in the name of the Client in a credit institution registered or having its place of business in a contracting state of the European Economic Area or in a country where requirements equal to those of Directive (EU) 2015/849 of the European Parliament and of the Council are in force;

9.5.6. gathering additional information and documents for the purpose of identifying the source and origin of the funds used in a transaction made in the business relationship in order to rule out the distensibility of the transactions;

9.6. Reassessment of a risk profile of a Client must be done not later than 6 months after establishment of Business Relationship.

9.7. After taking enhanced DD measures, the MB shall decide whether to establish or continue the Business Relationship with the Client in respect of whom the enhanced DD measures were taken.

9.8. If a Client who, by the date of entry into a contract, has not performed any prominent public functions for at least a year, and such person is deemed to pose no further risk specific to PEP, this Client is not considered as the PEP, therefore application of enhanced DD measures is not required.

9.9. The Representative may not apply enhanced DD measures stipulated in section 9.5 to local PEP, if there are no other circumstances leading to the higher risk.

10. Risk assessment

10.1. The Representative will establish a risk profile of a Client based on information gathered under the Rules.

10.2. The Provider of service applies the following risk categories:

i. Normal risk (the risk level is normal, there are no high risk characteristics present);
ii. High risk, which is sub categorized as High risk I and High risk II.

10.3. For every Client, who does not fall into the "normal risk" category, the Representative shall record the Client's risk category in the Provider of service's database of Clients and on the documents as "High risk I" or "High risk II". Only the CO shall have the right to change the risk category recorded for a Client.

10.4. Assessment of risk profile of natural persons

10.4.1. When establishing the risk category of a Client being a natural person, the country of residence of the Client, the region where the Client operates, and status of PEP shall be taken into account.

10.4.2. If there are several characteristics of the category "High risk I" present, or if, in addition to the characteristics of "High risk I", at least one of the "High risk II" characteristics is present, the Client shall be determined to be falling into the category "High risk II".

10.4.3. Characteristics of high risk in the case of a natural person, and the appropriate DD measures:

High risk category I	**DD measures**
The actual place of residence or employment or business of a Client is in a country, which is included in the list of risk countries (see Exhibit 1).	Ask the Client to provide additional information about the purpose of establishing the Business Relationship and his/her economic activities. Ask the Client to provide additional information about its links with the said foreign state.
The Client is associated with a PEP.	The decision is taken by the MB.
The Client is associated with a local PEP.	Conduct an internet search about the Client. Ask additional information and documents, which prove the legal origin of Client's assets. If there are no other circumstances leading to the higher risk and the MB approves, it is not required to apply enhanced DD measures stipulated in section 10.7.

High risk category II	**DD measures**
A person associated with the Client is a PEP.	Conduct an internet search about the Client. Ask additional information and documents, which prove the legal origin of Client's assets.
There is information that the Client is suspected to be or to have been linked with a financial offence or other suspicious activities.	Check information about International Sanctions (see also Section 15) or ask guidance from the CO. Ask additional information and documents, which prove the legal origin of the Client's assets.
The Client is related to a non-resident individual, whose place of residence or activities is in a country, which is listed in the list of risk countries (see Exhibit 1).	Ask the Client to provide additional documents to identify the Client and, if possible, check the Client's data vis-à-vis the previously presented documents and information. Verify and compare the data submitted by the Client against the additional documents, data or information, which originates from a reliable and independent source.

10.5. Assessment of risk profile of legal persons

10.5.1. When establishing the risk category of a legal person, assessment shall be based on the country of location of the legal person, its area of activity, the transparency of ownership structure and the management.

10.5.2. If there are several characteristics of the category "High risk I", or if, in addition to the characteristics of "High risk I", at least one of the "High risk II" characteristics is present, the Client shall be determined to be falling into the category "High risk II".

10.5.3. Characteristics of high risk in the case of a legal person, and the appropriate DD measures

High risk category I	DD measures
The Client is a legal person registered in the European Economic Area or in Switzerland, whose area of activity is associated with enhanced money-laundering risk (see Exhibit 1).	Ask the Client to provide additional documents to identify it and, if possible, check the Client's data vis-à-vis the previously presented documents and information. Verify and compare the data submitted by the Client against the additional documents or information, which originates from a reliable and independent source.
The Client is situated in a country, which is listed in the list of risk countries (see Exhibit 1).	Ask the Client to provide additional information about its links with the said foreign state. Ask for additional information about the purpose of establishing the Business Relationship.
The legal person is a non-profit association, trust, civil law partnership or another contractual legal arrangement, whose activities and liability are insufficiently regulated by law, and the legality of financing of which is not easy to screen.	Check the authenticity of the presented documents and verify the accuracy of the data. Ask for help from the CO. Ask the Client to provide information about relationships with other credit or financing institutions, and the opinion of the respective credit or financing institution. Ask additional information and documents, which prove the legal origin of the Client's assets.
The representative or the Beneficial Owner of a legal person is a local PEP or his or her family member.	Ask the Client to provide additional information about the need and purpose of establishing the Business Relationship. Ask the Client to provide information about relationships with other credit or financing institutions, and the opinion of the respective credit or financing institution about the Client. Conduct an internet search about the Client, being a legal person, and its Beneficial Owner. Ask additional information and documents, which prove the legal origin of the Client's assets. If there are no other circumstances leading to the higher risk and the MB approves, it is not required to apply enhanced DD measures stipulated in section 10.7.

High risk category II	DD measures
The representative or the Beneficial Owner of a legal person is a PEP or his or her family member.	Ask the Client to provide additional information about the need and purpose of establishing the Business Relationship. Ask the Client to provide information about relationships with other credit or financing institutions, and the opinion of the respective credit or financing institution about the Client. Conduct an internet search about the Client, being a legal person, and its Beneficial Owner. Ask additional information and documents, which prove the legal origin of the Client's assets.

	There is information that the person is suspected to be or to have been linked with a financial offence or other suspicious activities.	Check information about International Sanctions (see also Section 15) or ask guidance from the CO. Ask additional information and documents, which prove the legal origin of the Client's assets.
	A legal person registered outside the European Economic Area, whose field of business is associated with a high risk of Money Laundering (see Exhibit 1). A legal person registered outside the European Economic Area, who is operating outside the country of its registered location. A legal person is operating or is registered in a low tax rate country (see Exhibit 1) or the place of residence, place of registration of the legal person, its owners or Beneficial Owners, or the territory of business of the legal person is situated in a country listed in the list of risk countries (see Exhibit 1).	Ask the Client to provide additional information about its links with the said foreign state. Ask for additional information about the purpose of establishing the Business Relationship. Verify and compare the data submitted by Client against the additional documents, data or information, which originates from a reliable and independent source (if obtaining such information is possible). Ask additional information and documents, which prove the legal origin of the Client's assets.

10.6. The above listed DD measures can be combined, as appropriate, in respect to other listed or non-listed risks.

11. Registration and storage of data

11.1. The Representative shall ensure that Client data are registered in the Provider of service's Client database within the required scope.

11.2. Registration of data of a natural person

11.3. The following obtained data shall be recorded in the Provider of service's information system:

i. Name, personal ID code or, in the absence of the latter, date of birth and the address of the person's permanent place of residence and other places of residence;
ii. the name and number of the document used for identification and verification of the identity of the person, its date of issue and the name of the issuing authority;
iii. occupation, profession or area of activity – establish the area of activity (occupation) and the status of the person (trader, employee, student, pensioner);
iv. the Representative shall record information about whether
the person is performing or has performed prominent public functions, or is a close associate or family member of the person performing prominent public functions;
v. Citizenship and the country of tax residency;
vi. the origin of assets.

11.4. In case of a representative, the following info shall be recorded:

i. same as provided for in pints i-ii of Section 11.2.1;
ii. the name of the document used for establishing and verification of the right of representation, the date of issue and the name or name of the issuing party.

11.5. If the Business Relationship is established by the Client or the representative with the use of the ID card or other e-identification system, the data of the document used for identification is saved automatically in the digital signature. If identification takes place at a face-to-face meeting with the

Client, the data of the document used for identification is recorded on the copy of the identification document.

11.6. Registration of data of a Client who is a legal person

11.6.1. The following information on the Client being a legal person shall be recorded:

i. Name, legal form, registry code, address, date of registration and activity locations;
ii. information concerning means of communication and contact person(s);
iii. names of the members of the management board or an equivalent governing body, and their powers to represent the Client, and whether any of them is a PEP;
iv. information about the Beneficial Owners;
v. Field(s) of activity (i.e. the NACE codes);
vi. name and number of the document used for identification and verification of the identity, its date of issue and the name of the issuing authority;
vii. country of tax residency of the legal person (VAT number);
viii. date of registration of the legal person in the Provider of service's database;
ix. purpose of the Business Relationship;
x. origin of assets (normal business operations/other);

11.6.2. The following information about the Beneficial Owner shall be recorded:

i. Name, personal ID code or, in the absence of the latter, date of birth and place of residence;
ii. type of control over the enterprise (e.g. shareholder);
iii. is the person a PEP;
iv. information about the representative as set forth under 11.2.2.

11.6.3. If the Business Relationship is established by the representative of the Client with the use of the ID card or other e-identification system, the data of the document used for identification is saved automatically in the digital signature. If identification takes place at a face-to-face meeting with the representative of the Client, the data of the document used for identification is recorded on the copy of the identification document.

11.6.4. Information from the B-card, i.e. the legal representatives of the Client being a legal person stated on the B-card, shall be recorded on the Client data registration sheet or the contract concluded with the Client.

11.7. The Representative shall record all the data regarding:

11.7.1. Provider of service's decision to refuse establishment Business Relationship. The Representative shall record all the data, if, as a result of taking DD measures, a person refuses to establish the Business Relationship.

11.7.2. Impossibility to take DD measures due to information technology means;

11.7.3. Termination of the business relationship, as a result of impossibility to take DD measures;

11.8. Storage of Data

11.8.1. The respective data is stored in a written format and/or in a format reproducible in writing and, if required, it shall be accessible by all appropriate staff of the Provider of service (MB, Representatives, marketing, CO etc).

11.8.2. The originals or copies of the documents, which serve as the basis for identification of a person, and of the documents serving as the basis for establishing a Business Relationship, shall be stored for at least five (5) years following the termination of the Business Relationship.

11.8.3. The data of the document prescribed for the digital identification of a Client, information on making an electronic query to the identity documents database, and the audio and video recording of the procedure of identifying the person and verifying the person's identity shall be stored at least five (5) years following the termination of the Business Relationship.

11.8.4. Also to be stored:

i. manner, time and place of submitting or updating of data and documents;
ii. name and position of Representative who has established the identity, checked or updated the data.

12. Reporting

12.1. Notification of the CO

12.1.1. Any circumstances identified in the Business Relationship are unusual or suspicious or there are characteristics which point to Money Laundering, Terrorist Financing, or an attempt of the same the Representative shall promptly notify the CO.

12.1.2. The CO shall analyse and forward the respective information to the MB.

12.2. Notification of FIU

12.2.1. Before reporting any transaction connected with suspected Money Laundering or Terrorist Financing to the FIU, the CO shall analyse the content of the information received, considering the Client's current area of activity and other known information.

12.2.2. The CO shall decide whether to forward the information to the FIU and the MB shall decide whether to terminate the Business Relationship.

12.2.3. The CO shall make a notation "AML" behind the name of the Client in the Provider of service's Client database or on the documents, and shall notify the FIU promptly, but not later than within 2 business days after discovering any activities or circumstances or arising of suspicion, using the respective web-form for notifying the FIU. Copies of the documents as set forth by guidelines of FIU or further requested by FIU shall be appended to the notice.

12.2.4. The FIU shall be notified of any suspicious and unusual transactions where, including such where the financial obligation exceeding 32 000 euros or an equivalent amount in another currency is performed in cash, regardless of whether the transaction is made in a single payment or several related payments.

12.2.5. The CO shall store in a format reproducible in writing any reports received from the Representatives about suspicious circumstances, as well as all information gathered to analyse such notices, as well as other linked documents and notices to be forwarded to the FIU, along with the time of forwarding the notice, and the information about the Representatives who forwarded the same.

12.2.6. The Client who is reported to the FIU as being suspicious, may not be informed of the same.

12.2.7. It is also prohibited to inform any third persons, including other Representatives, of the fact that information has been reported to the FIU, and the content of the reported information, except for the MB/CO.

12.3. Termination of the Business Relationship with a Client in the event of suspected Money Laundering and Terrorist Financing

12.3.1. Pursuant to law, the Provider of service is obliged to extraordinarily and unilaterally terminate the Business Relationship without observing the advance notification period, if:

i. The Client fails to present upon identification or upon updating the previously gathered data or the taking of DD measures, true, full and accurate information, or
ii. The Client or a person associated with the Client does not present data and documents evidencing of the lawfulness of the economic activities of the Client, or
iii. the Provider of service suspects for any other reasons that the Client or the person associated with the Client is involved in Money Laundering or Terrorist Financing, or
iv. the documents and data submitted by the Client do not dispel the Provider of service's suspicions about the Client's possible links with Money Laundering or Terrorist Financing.

12.3.2. The decision on terminating the Business Relationship shall be taken by the Management Board, considering also the proposal of the CO.

12.3.3. The Client shall be notified of the termination of Business Relationship in writing, provided that it is consistent with Section 12.2.7. Notation about the cancellation of the Business Relationship shall be made in the Provider of service's Client database or documentation, and a note "AML" shall be added to the Client's data, provided that it is consistent with Section 12.2.8.

12.4. Indemnification of the Representatives

12.4.1. The Provider of service and its Representatives shall not, upon performance of the obligations arising from the Rules, be liable for damage arising from failure to carry out any transactions (by the due date) if the damage was caused to the persons in connection with notification of the FIU of the suspicion of Money Laundering or Terrorist Financing in good faith, or for

damage caused to a Client or in connection with the cancellation of a Business Relationship on the basis provided in Section 12.3.

12.4.2. Fulfilment of the notification obligation by the Representative acting in good faith, and reporting the appropriate information shall not be deemed breach of the confidentiality obligation imposed by the law or the contract, and no liability stemming from the legislation or the contract shall be imposed upon the person who has performed the notification obligation.

13. Implementation of International Sanctions

13.1. The Provider of service is required to implement International Sanctions in force.

13.2. Representatives shall draw special attention to all its Clients (present and new), to the activities of the Clients and to the facts which refer to the possibility that the Client is a subject to International Sanctions. Control and verification of possibly imposed International Sanctions shall be conducted by the Representatives as part of DD measures applied to the Clients in accordance with these Rules.

13.3. The Representatives who have doubts or who know that a Client is subject to International Sanctions, shall immediately notify the CO. In case of doubt, if the CO finds it appropriate, the Representative shall ask the Client to provide additional information that may help to identify whether he/she is subject to International Sanctions or not.

13.4. The CO shall be responsible for the implementation of International Sanctions.

13.4.1. The CO shall:

i. regularly follow the webpage of FIU (https://www.politsei.ee/et/rahapesu/) and immediately take measures provided for in the act on the imposition or implementation of International Sanctions;
ii. upon entry into force of an act on the imposition or implementation of International Sanctions, the amendment, repeal or expiry thereof, immediately check whether any of the Clients is subject to International Sanctions with regard to whom the financial sanction is imposed, amended or terminated;
iii. if an act on the imposition or implementation of International Sanctions is repealed, expires or is amended in such a manner that the implementation of International Sanctions with regard to the subject of International Sanctions is terminated wholly or partially, terminate the implementation of the measure to the extent provided for in the act on the imposition or application of International Sanctions;
iv. keep an updated record of subjects of International Sanctions and submit this information to the Representatives in the form that allows to use this information in the course of their activity;
v. provide training to the Representatives that allows them to establish independently the subjects of International Sanctions;
vi. assist the Representatives if they have doubt or knowledge that a Client is a subject to International Sanctions;
vii. supervise the application of the Rules regarding the implementation of International Sanctions by the Representatives;
viii. review and keep updated the Rules regarding the implementation of International Sanctions
ix. notify FIU of Clients who are subject to International Sanctions or in part of whom the CO, the Representatives have doubts;
x. keep record of made checks, notifications submitted to FIU and applied measures in part of detected subjects to International Sanctions.

13.4.2. When making checks on Clients as to detect whether they are subject to International Sanctions, the following information shall be recorded and preserved for five years:

i. Time of inspection;
ii. Name of person who carried out inspection;
iii. Results of inspection;
iv. Measures taken.

13.4.3. If in the course of the check, it shall be detected that a Client or a person who used to be a Client is subject to International Sanctions, the CO shall notify the Representatives who dealt with this Client, the Management Board and FIU. The notification shall be submitted at least in the way that allows its reproduction in writing.

13.4.4. The Client who is subject to International Sanctions and about whom the notification is made, shall not be informed of the notification.

13.4.5. Application of special measures and sanctions on the Client who is detected to be subject to International Sanctions should be authorized by FIU.

13.4.6. When making checks of Clients, the possible distorting factors in personal information (i.e. way of written reproduction of name etc.) must be kept in mind.

14. Training

14.1. The Provider of service shall ensure that all Representatives who have contacts with Clients or matters involving Money Laundering are provided with regular training and information about the nature of the Money Laundering and Terrorist Financing risks, as well as any new trends within the field. The CO shall arrange regular training concerning prevention of Money Laundering and Terrorist Financing to explain the respective requirements and obligations.

14.2. Initial training is provided at the start of representative service. The Representatives who are communicating with the Clients directly may not start working before they have reviewed and committed to the adherence of these Rules or participated in the Money Laundering and Terrorist Financing prevention training.

14.3. Training is provided regularly, at least once a year, to all Representatives and other relevant designated staff of the Provider of service. Training may be provided also using electronic means (conference calls, continuous email updates provided confirmation on receipt and acceptance is returned and similar means).

14.4. Training materials and information shall be stored for at least three years.

15. Internal audit and amendment of the Rules

15.1. Compliance with the Rules shall be inspected at least once a year by the CO, whose job duties are set out in Section 4.1.

15.2. The report on the results of the inspection concerning the compliance with the measures for prevention of Money Laundering and Terrorist Financing shall set out the following information:

- **i.** time of the inspection;
- **ii.** name and position of the person conducting the inspection;
- **iii.** purpose and description of the inspection;
- **iv.** analysis of the inspection results, or the conclusions drawn on the basis of the inspection.

15.3. If the inspection reveals any deficiencies in the Rules or their implementation, the report shall set out the measures to be applied to remedy the deficiencies, as well as the respective time schedule and the time of a follow-up inspection.

15.4. If a follow-up inspection is carried out, the results of the follow-up inspection shall be added to the inspection report, which shall state the list of measures to remedy any deficiencies discovered in the course of the follow-up inspection, and the time actually spent on remedying the same.

15.5. The inspection report shall be presented to the MB, who shall decide on taking measures to remedy any deficiencies discovered.

***

v.**Form 1**

Client Data

Updated:	Risk category

Client data sheet ('know your customer)

Name, address, etc.	Name	
	Personal code/Date of birth/Registry code	
	Address/Location	
	Citizenship (in case of natural person)	
	Occupation, area of activity	
	Name and date of issuance of document used for identification (in case of natural person and representative of legal person)	
	Name and number of the document used for identification and verification of the identity of a foreign legal person	
	Postal code and city	
	The country of tax residency	
	Area of activity (in case of legal person)	
	E-mail	Telephone
	Contact person and email	Telephone
	Have the securities of the company been accepted for trading on a regulated securities market? (in case of legal person) NO YES, if Yes, then on which securities market?	

<table>
<tr><td rowspan="11">Beneficial Owner</td><td colspan="2">Record the Beneficial Owners:
A Beneficial Owner is a natural person who:
i. Taking advantage of his influence, exercises control over a transaction, operation or another person and in whose interests or favour or on whose account a transaction or operation is performed taking advantage of his influence, makes a transaction, act, action, operation or step or otherwise exercises control over a transaction, act, action, operation or step or over another person and in whose interests or favour or on whose account a transaction or act, action, operation or step is made.
ii. Ultimately owns or controls a legal person through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that person, including through bearer shareholdings, or through control via other means. Direct ownership is a manner of exercising control whereby a natural person holds a shareholding of 25 per cent plus one share or an ownership interest of more than 25 per cent in a company. Indirect ownership is a manner of exercising control whereby a company which is under the control of a natural person holds or multiple companies which are under the control of the same natural person hold a shareholding of 25 per cent plus one share or an ownership interest of more than 25 per cent in a company.
iii. Holds the position of a senior managing official, if, after all possible means of identification have been exhausted, the person specified in clause ii cannot be identified and there is no doubt that such person exists or where there are doubts as to whether the identified person is a beneficial owner.
iv. In the case of a trust, civil law partnership, community or legal arrangement, the beneficial owner is the natural person who ultimately controls the association via direct or indirect ownership or otherwise and is such associations': settlor or person who has handed over property to the asset pool, trustee or manager or possessor of the property, person ensuring and controlling the preservation of property, where such person has been appointed, or the beneficiary, or where the beneficiary or beneficiaries have yet to be determined, the class of persons in whose main interest such association is set up or operates.</td></tr>
<tr><td colspan="2">Does the company have Beneficial Owners:
YES NO, if No, please explain:</td></tr>
<tr><td>Name</td><td>Personal ID code/ DOB</td></tr>
<tr><td rowspan="2">Place of residence</td><td>Citizenship</td></tr>
<tr><td>Shareholding (%)</td></tr>
<tr><td>Name</td><td>Personal ID code/ DOB</td></tr>
<tr><td rowspan="2">Place of residence</td><td>Citizenship</td></tr>
<tr><td>Shareholding (%)</td></tr>
<tr><td>Name</td><td>Personal ID code/ DOB</td></tr>
<tr><td rowspan="2">Place of residence</td><td>Citizenship</td></tr>
<tr><td>Shareholding (%)</td></tr>
</table>

Members of the MB (in case of legal person)	Name	Personal ID code/ DOB	
	Place of residence	Copy of the ID document appended YES	Valid till
	Name	Personal ID code/ DOB	
	Place of residence	Copy of the ID document appended YES	Valid till
	Name	Personal ID code/ DOB	
	Place of residence	Copy of the ID document appended YES	Valid till

Authorised persons (representatives)	Name	Personal ID code/ DOB	
	Place of residence	Copy of the ID document appended YES	Valid till
		Power of attorney appended YES	Valid till
	Name	Personal ID code/ DOB	
	Place of residence	Copy of the ID document appended YES	Valid till
		Power of attorney appended YES	Valid till
	Name	Personal ID code/ DOB	
	Place of residence	Copy of the ID document appended YES	Valid till
		Power of attorney appended YES	Valid till

Purpose of the Business Relationship	Please specify

<table>
<tr><td>Identification of Politically Exposed Persons (to be filled if relevant)</td><td colspan="3">Record on the Beneficial Owners, members of the MB or authorised representative a Politically Exposed Person.

A Politically Exposed Person is a natural person who is or who has been entrusted with prominent public functions including a head of state, head of government, minister and deputy or assistant minister; a member of parliament or of a similar legislative body, a member of a governing body of a political party, a member of a supreme court, a member of a court of auditors or of the board of a central bank; an ambassador, a chargé d'affaires and a high-ranking officer in the armed forces; a member of an administrative, management or supervisory body of a state-owned enterprise; a director, deputy director and member of the board or equivalent function of an international organisation, except middle-ranking or more junior officials.
• The provisions set out above also include positions in the European Union and in other international organizations.
• A family member of a person performing prominent public functions is the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person; a child and their spouse, or a person considered to be equivalent to a spouse, of a politically exposed person; a parent of a politically exposed person.
• A close associate of a person performing prominent public functions is a natural person who is known to be the beneficial owner or to have joint beneficial ownership of a legal person or a legal arrangement, or any other close business relations, with a politically exposed person; and a natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person.
YES
NO
If Yes, please record the person's name, position (occupation) and links with the politically exposed person.</td></tr>
<tr><td></td><td>Name</td><td>Position (occupation)</td><td>Link</td></tr>
<tr><td></td><td>Name</td><td>Position (occupation)</td><td>Link</td></tr>
</table>

vi.Exhibit 1

Exhibit 1a. Contracting states of the European Economic Area

Please refer to http://elik.nlib.ee/pohifakte-euroopa-liidust/liikmesriigid-euroopa-majanduspiirkonna-riigid/

Exhibit 1b. Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies (Text with EEA relevance)

Please refer to https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.254.01.0001.01.ENG

Exhibit 1c. List of risk countries (countries which according to FATF does not follow requirements of prevention of Money Laundering and Terrorism Financing)

Please refer to: http://www.fatf-gafi.org/countries/#high-risk

Exhibit 1c. List of risk countries (countries which according to the FIU are under big threat of terrorism)

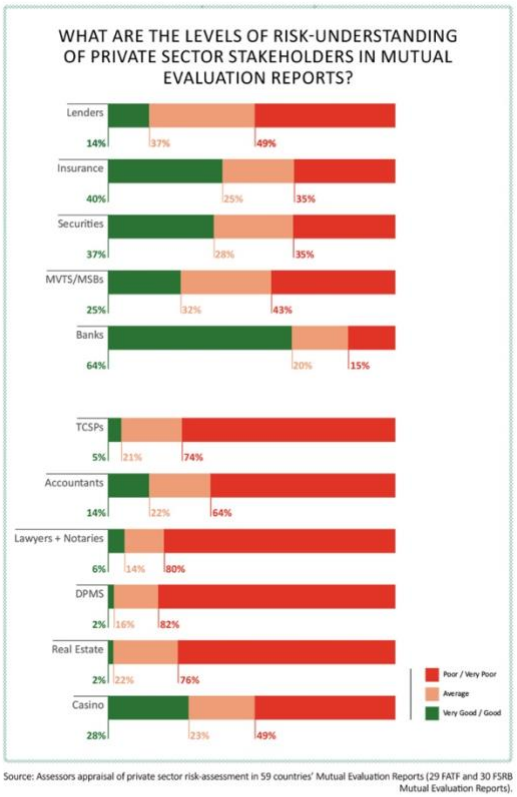
Afghanistan, Algeria, United Arab Emirates, Bahrein, Bangladesh, Egypt, Indonesia, Iraq, Iran, Yemen, Jordanian, Qatar, Kuwait, Lebanon, Libya, Malaysia, Mali, Morocco, Mauritania, Nigeria, Oman, Pakistan, Palestine, Saudi Arabia, Somalia, Sri Lanka, Sudan, Syria, Tunisia, Turkey, Ethnic groups of Caucasus belonging to Russian Federation (chechens,lesgid, ossetians, ingushes etc.)

Exhibit 1d. List of countries that are NOT regarded as low tax rate countries

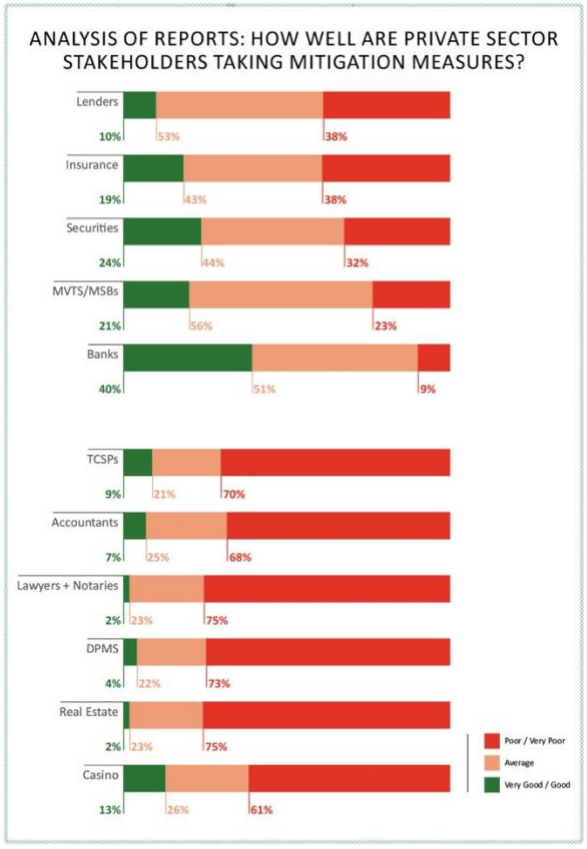
https://www.emta.ee/et/ariklient/tulud-kulud-kaive-kasum/mitteresidendi-eesti-tulu-maksustamine/nimekiri-territooriumidest

Source: LEIpapa OÜ

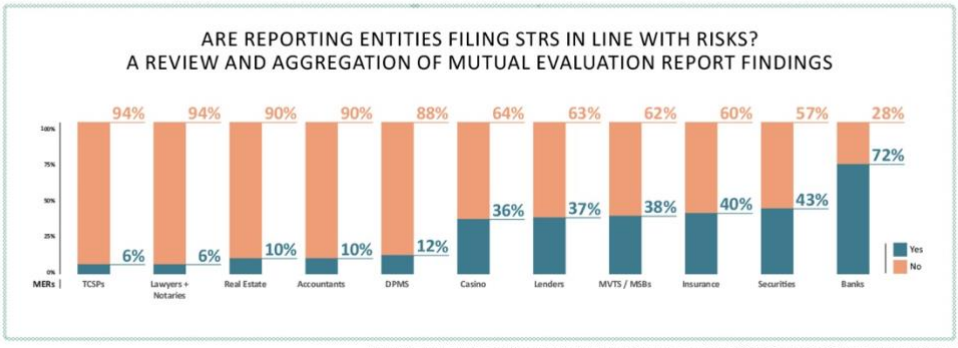
Appendix 8. Figures from the Report on the State of Effectiveness and Compliance with the FATF Standards



Source: Assessors appraisal of private sector risk-assessment in 59 countries' Mutual Evaluation Reports (29 FATF and 30 FSRB Mutual Evaluation Reports).



Source: Assessors appraisal of private sector risk-mitigation in 59 countries' Mutual Evaluation Reports (29 FATF and 30 FSRB Mutual Evaluation Reports).



Source: Assessors appraisals in 59 countries' mutual evaluation reports consisting of 29 FATF and 30 FSRB Mutual Evaluation Reports

Source: (FATF, 2022d, 28–29)

Appendix 9. Sample of the table for determination of the Client's risk profile

Risks category/score	**Low (1)**	**Medium (2)**	**High (3)**	**Prohibited (4)**	**Coefficient**	**Result**
Risks relating to Clients					2	
Risks relating to countries, geographic areas, or jurisdictions:					1	
Risks relating to products, services, or transactions					2	
Risks relating to communication, mediation or products, services, transactions, or delivery channels between the Registration Agent and the Client;					1	
The parameters for determining the risk profile of the Client are: The Client's risk profile is **<u>low</u>**, if **x < 2** The Client's risk profile is **<u>medium</u>**, if **2 ≤ x ≤ 3** The Client's risk profile is **<u>high</u>**, if **x > 3** The Client's risk profile is **<u>prohibited</u>** if at least one of the risks categories has 4 points. Exceptions: • Client's risk level may be determined as "low" only if no one of the risks categories scored as "high" or "prohibited". • Client's risk level shall be determined as "high" if at least one of the risks categories scored as "high".					**Average result (x):** **The risk level of the Client**	

Source: Compiled by the author based on the (Basel Committee on Banking Supervision (BCBS), 2020, 8-10)

Appendix 10. The list of unacceptable countries

- Afghanistan
- Burundi
- The Central African Republic
- The Democratic Republic of the Congo
- Eritrea
- Ethiopia
- Guinea
- Guinea-Bissau
- Iran
- Iraq
- Ivory Coast
- Lebanon
- Libya
- Mali
- Myanmar
- Nicaragua
- North Korea
- Somalia
- South Sudan
- Sri Lanka
- Sudan
- Syria
- Tunisia
- US Virgin Islands
- Venezuela
- Yemen
- Zimbabwe

Source: Compiled by the author

Appendix 11. Internal rules and procedures of LEIpapa OÜ (extract)

12. IDENTIFICATION OF PERSON USING INFORMATION TECHNOLOGY MEANS

12.1. When using information technology (IT) means to identify the person and to verify the person's identity data in accordance with clause 11.2, the natural person or the representative of a legal person, who wants to establish a business relationship, must use the following:

12.1.1. document intended for the digital identification of a person or other high-confidence e-identification system, which has been added to the list published in the Official Journal of the European Union based on Article 9 of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, pp. 73–114);

12.1.1.1. Where a person is a foreign national, the identity document issued by the competent authority of the foreign country must be used for the identification of the person and verification of data in addition to the means specified in clause 12.1.1.

12.1.2. an information technology means with a working camera, microphone and necessary hardware and software for digital identification, as well as internet connection with adequate speed.

12.2. In addition, information from a reliable and independent source is used to verify the identity using IT means. Obliged entity has the right to use the identification data entered in the database of identity documents in order to establish identity and verify the data.

12.3. Means and identification procedure provided for in clause 12.1 must meet the following requirements:

12.3.1. the information system must allow for digital identification of a person and digital signing;

12.3.2. the obliged person must verify the quality of its own and, if possible, the customer's information flow and ensure that the transmission of clear, recordable and reproducible synchronized sound and image, which is sufficient to understand the transmitted content unambiguously and reliably, is guaranteed;

12.3.3. the information flow containing image and sound is transmitted in real time;

12.3.4. the information flow that contains image and sound must be recorded with the time stamp, the customer's IP address, the personal identification code of the person to be identified, if there is no personal identification code, then the birth date and place and country of residence, whilst the time stamp must be tied to the data concerning it in such a manner that any later changes in data, the person who made the changes, and the time, manner and reason thereof can be identified;

12.3.5. Upon identification of a person and verification of person's identity data with IT means, the person's head and shoulders must be visible and framed. The face must be clear of shadows and uncovered, and clearly distinguishable from the background and other objects, and recognisable.

12.3.6. the person must have a possibility to change his or her body position and place themselves and the document in the frame to make it possible to identify the person and verify person´s identity, including viewing the data or images on the document.

12.4. The obliged entity has the right to require the change of body position and the removal of items covering the head or face and glasses or compliance with any other

instructions of the obliged entity given in order to guarantee the identification of a person and verification of person's identity data.

12.5. The obliged entity must publish information about the technical conditions for the identification of a person and verification of person's identity with information technology means. At least the following facts must be presented in the published information:

12.5.1. a reference to the applicable legislative provisions;

12.5.2. the information that the identification of a person and verification of person's identity with information technology means take place according to the procedure set out in applicable legislation;

12.5.3. a warning that the identification of a person and verification of person's identity does not oblige the obliged entity to establish a business relationship or guarantee the accessibility of services;

12.5.4. the conditions in the event of which the identification of a person and verification of person's identity with information technology means is considered unsuccessful.

12.6. Before the identification of a person and verification of person's identity with IT means, the obliged entity is obligated to notify the person of the provisions set out in clause 12.5 and to receive confirmation that the person has received the notification. Additionally, the person to be identified is obligated to agree to the conditions of the identification of a person and verification of person's identity, by confirming the following;

12.6.1. the person carries out the procedure personally, except for the cases where the participation of third persons is necessary to solve technical problems;

12.6.2. the data submitted by him or her during the interview specified in clause 12.15 is correct and complete and he or she is aware of the consequences associated with the submission of incorrect, misleading or incomplete information upon the establishment of a business relationship;

12.6.3. he or she meets the conditions established by the service provider for the establishment of business

12.7. In addition to the obligations set out in clause 12.5, a natural person or legal representative of a legal entity who uses the e-resident's digital identity card or other high-reliability e-identification system must also:

12.7.1. agree with the application of Estonian law;

12.7.2. show to the obliged entity in front of the camera the personal data page of the valid travel document issued by the foreign country.

12.8. The identification of a person and verification of person's identity using information technology means upon the establishment of a business relationship is considered unsuccessful if:

12.8.1. the natural person or the legal representative of a legal entity has intentionally submitted data that do not correspond to the identification data entered in the identity documents database or do not coincide with the information or data obtained with other procedures;

12.8.2. the session expires or is interrupted during the identification of a person, the identification questionnaire or the interview, or the information flow that transmits synchronized sound and image does not comply with the requirements set out in clause 12.3. The session expires when the natural person or the legal representative of the legal entity has not completed any activities in the service provider's information system during a period of 15 minutes;

12.8.3. the natural person or the legal representative of a legal entity has not given the confirmations prescribed in clauses 12.15 and 12.6;
12.8.4. the natural person or the legal representative of a legal entity refuses to comply with the obliged entity's instructions specified in clause 13.3;
12.8.5. the natural person or the legal representative of a legal entity uses the assistance of another person without the obliged entity's permission;
12.8.6. there are circumstances that give rise to suspicions of money laundering or terrorist financing.
12.9. In the event of circumstances prescribed in clauses 12.8.1 or 12.8.6, the obliged entity must send a notification thereof to the Financial Intelligence Unit.
12.10. The identification of a person and verification of person's identity using IT means takes place in the form of an identification questionnaire or an interview. On the basis of the collected data, the obliged entity prepares the customer profile of the person to be identified and the risk profile as a part thereof. The customer profile and the risk profile is prepared by the obliged entity in a form reproducible in writing.
12.11. The fulfilment of the preconditions of identification of a person and verification of person's identity data and the identification questionnaire are carried out by an employee of the obliged entity, a partner of the obliged entity or an automated system. The obliged entity is obligated to take measures in order to prevent the risks of the automated system being manipulated.
12.12. The identification questionnaire is used to ascertain the following:
12.12.1. In case of a natural person:
12.12.1.1. natural person's residential address;
12.12.1.2. connection of the legal entity's business;
12.12.1.3. if appropriate:
12.12.1.3.1. the beneficial owner;
12.12.1.3.2. whether the person is a politically exposed person;
12.12.1.3.3. other important information.
12.12.2. In case of a legal entity:
12.12.2.1. legal entity's business name;
12.12.2.2. registry code;
12.12.2.3. location and places of operation;
12.12.2.4. entity's legal form;
12.12.2.5. legal capacity;
12.12.2.6. lawful and contractual representatives;
12.12.2.7. beneficial owner(s);
12.12.2.8. if appropriate:
12.12.2.8.1. whether the beneficial owner is a politically exposed person;
12.12.2.8.2. main and secondary areas of activity;
12.12.2.8.3. other important information.
12.13. The employee of the obliged entity must assess the answers given in the identification questionnaire and record his or her opinion and the circumstances that are the basis thereof in the customer profile and risk profile specified in clause 12.10.
12.14. The obliged entity may waive a separate identification questionnaire if the information specified in clause 12.12 is collected and the requirements specified in clause 12.13 are complied with in the course of the interview.
12.15. In order to collect and verify the information and data required for the determination of the customer profile, the employee of the obliged entity carries out an interview, during which the employee asks partly structured questions, proceeding from the

results of the identification questionnaire. If the interview is carried out with the questionnaire, at least the data specified in clause 12.12 must be acquired with the questions.

12.16. The employee of the obliged entity if need may carry on the interview that is mandatory for the establishment of a business relationship in real time. The employee of the obliged entity must assess the customer's reaction during the interview, the reliability of the obtained information and data and compliance with the information and data obtained with other procedures, and record his or her opinion and the circumstances that are the basis thereof in the customer profile and risk profile specified in clause 12.10.

12.17. The information acquired during the questionnaire and the interview must be verified and preserved in accordance with the requirements set out for the application of due diligence measures and the procedures set out in these guidelines related to registration, verification and preservation of data.

13. IDENTIFICATION OF REPRESENTATIVE

13.1. The obliged entity identifies the customer and, where relevant, their representative and retains the following data on the person and, where relevant, their representative:

13.1.1. first and last name(s);

13.1.2. personal identification code or, if none, the date of birth

13.1.3. the place of residence or seat;

13.1.4. information on the identification and verification of the right of representation and scope thereof and, where the right of representation does not arise from law, the name of the document serving as the basis for the right of representation, the date of issue, and the name of the issuer.

13.2. The employee makes a copy of the personal data and of the page including the photograph of the identity document for preservation. Preservation date should be attached to the copy. Where the identified person has a valid document specified in clause 13.3 or an equivalent document, the person is identified and the person's identity is verified on the basis of the document or using means of electronic identification and trust services for electronic transactions, and the validity of the document appears from the document or can be identified using means of electronic identification and trust services for electronic transactions, no additional details on the document need to be retained.

13.3. The following valid documents may be used as the basis for the identification of a natural person:

13.3.1. an identity card;

13.3.2. a digital identity card;

13.3.3. a residence permit card;

13.3.4. an Estonian citizen's passport;

13.3.5. an alien's passport;

13.3.6. a temporary travel document;

13.3.7. a travel document for a refugee;

13.3.8. a driving permit issued in the Republic of Estonia;

13.3.9. a driving permit issued in a foreign country if the document includes user's name, photograph or facial image, signature or image of a signature and date of birth or personal identification code;

13.3.10. a travel document issued in a foreign country.

13.4. Where the original document specified in clause 13.3 is not available, the identity can be verified on the basis of a document specified in clause 13.3, which has been authenticated by a notary or certified by a notary or officially, or on the basis of other information originating from a credible and independent source, including means of electronic identification and trust services for electronic transactions, thereby using at least two different sources for verification of data in such an event.

13.5. The obliged entity verifies the correctness of the data specified in clause 13.1, using information originating from a credible and independent source for that purpose.

13.6. During the verification of the data from a credible and independent source obtained during the identification of a natural person and representative, in accordance with clause 11.4,

13.6.1. one of the sources is always:

13.6.1.1. an identity document with a photo specified in clause 13.3 or a colored and legible copy/image of this document; or

13.6.1.2. data and a photo of the person on the same document obtained from reliable and independent sources; or

13.6.1.3. the information (at least the name and personal identification code or the date and place of birth if there is no personal identification code) obtained in the course of strong authentication carried out with a digital personal identification tool if the money laundering and terrorist financing risk associated with the customer and the business relationship is lower than usual.

13.6.2. The following information obtained from a reliable and independent source may be the second source:

13.6.2.1. another document that complies with the conditions specified in subclauses 1 or 2 of clause 13.6.1 (a copy thereof or the data and photo obtained therefrom); or

13.6.2.2. the information (at least the name and personal identification code or the date and place of birth if there is no personal identification code) obtained in the course of strong authentication carried out with a digital personal identification tool; or

13.6.2.3. verification of the data directly related to a person via the Population Register or an equivalent register, provided that the source is a reliable and independent source within the meaning of clause 11.4 of these guidelines; or

13.6.2.4. information received from a first payment; or

13.6.2.5. other biometric data (fingerprint, facial image) or other information; or

13.6.2.6. information for checking the data directly associated with the person (e.g. place of work, residence or study).

13.7. In the case of representation, the obliged entity must also identify and verify the nature and scope of the right of representation. If the right of representation does not arise from law, the name, date of issue and name of issuer of the document that serves as a basis for the right of representation must be ascertained and retained. The obliged entity must observe the conditions of the right of representation granted to the representatives and provide services only within the scope of the right of representation.

13.8. The representative of a foreign legal entity must submit, on the request of the obliged entity, a document that proves their authorization and has been certified by a notary or in an equivalent manner and that has been legalized or certified with a certificate that replaces legalization (Apostille), unless otherwise stipulated in the international agreement.

13.9. When the right of representation of authorized and legal representatives is handled, it must be ascertained whether the representative knows their customer. In order to ascertain the nature of the actual relationships between the representative and the represented person, the representative must know the content and objective of the declarations of intent of the person they represent, and they must also be able to answer other relevant questions about the represented person's location, areas of activity, turnover and transaction partners, other related persons and beneficial owners. The representative must also confirm that they are aware of and convinced about the source and legal origin of the funds used by the represented person in the transaction.

14. IDENTIFICATION OF LEGAL ENTITY

14.1. The obliged entity identifies the legal entity and retains the following data regarding the entity:

14.1.1. business name or name (with the legal form) of the legal entity;

14.1.2. registry code or registration number and date;

14.1.3. name of the director or names of members of the management board or members of another equivalent body, and their authorities in representing the legal entity, whereby the representative who wants to establish a customer relationship is identified and the obtained data are verified according to the requirements of these guidelines;

14.1.4. also the collection and retention of other data directly related to the entity, such as:

14.1.4.1. location of the legal entity, whereby the theory of the country of establishment must be proceeded from;

14.1.4.2. place of business of the legal entity;

14.1.4.3. data of the means of communication of the legal entity.

14.2. The following documents are used for identification of the legal entity:

14.2.1. registry card of the relevant register;

14.2.2. registration certificate of the relevant register; or

14.2.3. a document equivalent with an aforementioned documents or relevant documents of establishment of the legal entity.

14.3. The obliged entity verifies the correctness of the data specified in clause 14.1, using information originating from a credible and independent source for that purpose. Where the obliged entity has access to the commercial register, register of non-profit associations and foundations or the data of the relevant registers of a foreign country, the submission of the documents specified in clause 14.2 does not need to be demanded from the customer.

14.4. Where the original document specified in clause 14.2 is not available, the identity can be verified on the basis of a document specified in clause 14.2, which has been authenticated by a notary or certified by a notary or officially, or on the basis of other information originating from a credible and independent source, including means of electronic identification and trust services for electronic transactions, thereby using at least two different sources for verification of data in such an event.

14.5. During the verification of the data from a credible and independent source obtained during the identification of a legal entity, in accordance with clause 11.4, the source shall be considered credible and independent when the obliged entity:

14.5.1. sees the original of the document specified in clause 14.2;

14.5.2. sees a copy of the document specified in clause 14.2 that has been authenticated by a notary, certified by a notary or officially certified; or

14.5.3. has access to the data in the commercial register, register of non-profit associations and foundations or the relevant registers of foreign countries via a computer network.

14.6. The documents specified in clause 14.2 must be issued by a competent authority or body not earlier than six months before their submission to the obliged entity.

14.7. In situations not specified in clause 14.2, the reliable and independent source is verification of the information obtained in the course of identification which originates from two different sources and complies with the requirements specified in clauses 11.4.1-11.4.3. Provisions of clause 14.5 must be applied in situations where the representative of a legal entity must be identified face-to-face according to clause **Error! Reference source not found.**.

14.8. Within the meaning of clause 11.4, two different sources during the identification of a legal entity means that the data medium, place or measure of obtaining information must be different (i.e. it cannot be the same data medium).

14.9. In addition to the document specified in clause 14.2 (if the obliged entity does not select two different identity documents of the customer for verification), the second source may also be information obtained from a reliable and independent source for checking the data directly related to the person (such as the location, etc.).

14.10. Public documents use to identify a legal entity issued in a foreign country must be legalized or confirmed with a certificate replacing legalization (apostille) unless otherwise provided for in an international agreement.

14.11. In the case of documents in foreign languages, the obliged entity has the right to demand translation of the documents to a language they understand. The use of translations should be avoided in situations where the original documents are prepared in a language understandable to the obliged entity.

15. BENEFICIAL OWNER AND THEIR IDENTIFICATION

15.1. Upon the establishment of a business, the obliged entity must identify the beneficial owner of the customer or the person participating and take measures to verify the identity of the beneficial owner to the extent that allows the obliged entity to make sure that they know who the beneficial owner is.

15.2. The beneficial owner means a natural person who, taking advantage of their influence, makes a transaction, act, action, operation or step or exercises control in another manner over a transaction, act, action, operation or step or over another person and in whose interests or for whose benefit or on whose account a transaction or act, action, operation or step is made. In the case of a legal entity, the beneficial owner is a natural person whose direct or indirect holding, or the sum of all direct and indirect holdings in the legal person, exceeds 25 percent, including holdings in the form of shares or other forms of bearer.

15.3. The obliged entity must understand the ownership and control structure of the customer or the upon the establishment of a business.

15.4. The beneficial owner does not have to be identified:

15.4.1. in the case of a company listed on a regulated market that is subject to disclosure requirements consistent with European Union law or subject to equivalent international standards which ensure adequate transparency of ownership information;

15.4.2. in the case of an apartment association provided for in the Apartment Ownership and Apartment Associations Act;

15.4.3. in the case of a building association provided for in the Building Association Act;

15.4.4. in the case of a company whose securities are traded on a regulated securities market.

15.5. The beneficial owner of a legal entity is identified in stages where the obliged entity proceeds to each subsequent stage if the beneficial owner of the legal entity cannot be determined in the case of the previous stage. The stages and questions are as follows:

15.5.1. is it possible to identify, in respect of the customer that is a legal entity or a person participating in the transaction, the natural person or persons who actually ultimately control the legal entity or exercise influence or control over it in any other manner, irrespective of the size of the shares, voting rights or ownership rights or its direct or indirect nature;

15.5.2. whether the customer that is a legal entity or the person participating in the transaction has a natural person or persons who own or control the legal entity via direct or indirect shareholding. Family connections and contractual connections must also be taken into account here;

15.5.3. who is the natural person in senior management, who must be defined as the beneficial owner, as the answers to the previous two questions have not made it possible for the obliged entity to identify the beneficial owner.

15.6. Direct ownership is a manner of exercising control whereby the natural person owns a 25 percent shareholding plus one share or an ownership right of over 25 percent in the company.

15.7. Indirect ownership is a manner of exercising control whereby a 25 percent shareholding plus one share or an ownership right of over 25 percent in the company is owned by a company that is controlled by a natural person or several companies that are controlled by the same natural person.

15.8. A member of senior management specified in clause 15.5.3 is a person who:

15.8.1. makes the strategic decisions that fundamentally affect business activities and/or practices and/or the company general (business) trends; or in its absence

15.8.2. carries out everyday or regular management functions of the company within the scope of executive power (e.g. chief executive officer (CEO), chief financial officer (CFO), director or president, etc.).

15.9. Where, after all possible means of identification have been exhausted, the person specified in clause 15.2 cannot be identified and there is no doubt that such person exists or where there are doubts as to whether the identified person is a beneficial owner, the natural person who holds the position of a senior managing official is deemed as a beneficial owner.

15.10. The obliged entity may consider beneficial owner to be a person who in some other way exercises control over the company without owning a 25 percent shareholding in that company. This situation also arises when the obliged entity suspects that some third person exercises significant control over the company whose ties to the company can not be legally proven or this proof is difficult to obtain. In such a situation, information must be demanded about the shareholders, partners and other persons who exercise control or other significant influence over the activities of the legal entity.

15.11. In the case of a trust or association of persons that does not have the status of a legal entity, the beneficial owner is the natural person who ultimately controls the association via direct or indirect ownership or otherwise and who is the association's:

15.11.1. settlor or person who has handed over property to the asset pool;

15.11.2. trustee, asset manager or possessor;

15.11.3. person ensuring and controlling the preservation of assets, where such person has been appointed;

15.11.4. the beneficiary, or where the beneficiary or beneficiaries have yet to be determined, the class of persons in whose main interest such association is set up or operates;

15.11.5. any other person who in any way has ultimate control of a trust or of the assets of the association.

15.12. The obliged entity takes measures to verify the identified beneficial owner and does the same to an extent that makes it possible for the obliged entity to conclude that they know who the beneficial owner is. In the case of legal entities, this requires, in the case of identifying the purpose and nature of the business relationship, making it possible to conclude that the customer's beneficial owner, if the latter participates actively in the company's activities, is capable of operating in the declared area of activity, with the declared scope of activity and with the declared main business partners and has the required experience; and that the obliged entity:

15.12.1. sees the original of the document specified in clause 14.2;

15.12.2. has access to the data in the commercial register, register of non-profit associations and foundations or the relevant registers of foreign countries via a computer network and checks the beneficial owner's data in said register;

15.12.3. sees a copy of the document specified in clause 14.2 that has been certified by a notary or officially certified;

15.12.4. uses other publicly accessible and/or reliable sources that are sufficient to make it possible to conclude who the beneficial owner is.

15.13. If the identity documents of the legal entity or the other submitted documents do not indicate directly who the beneficial owner of the legal entity is, the relevant data (incl. data about being a member of a group and the ownership and management structure of the group) are registered on the basis of the statement of the representative of the legal entity or the document written by hand by the representative of the legal entity. Reasonable measures must be taken to verify the accuracy of the information established on the basis of statements or a handwritten document (e.g. by making inquiries in the relevant registers), requiring the submission of the legal entity's annual report or other relevant document.

15.14. If the obliged entity has doubts about the accuracy or completeness of the relevant information, the obliged entity shall verify the information provided from publicly available sources and, if necessary, request additional information from the person.

15.15. When determining the beneficial owner, particular attention must be paid to companies established in low-tax areas whose legal capacity is not always clear.

15.16. In the case of a trust or other similar legal entity, assertation must be obtained about the nature of the beneficial owner on the basis of the civil law partnership agreement, letter of wishes, trust deed and other documents in addition to publicly accessible and/or reliable data. The provisions of clause 15.3 must be applied if the obliged entity wants to use the statement or handwritten document of the beneficial owner.

15.17. If another legal person has control over a legal person in accordance with the definition of beneficial owner, the obliged entity must assess the risk of the person

or customer and collect data on other legal persons related to other persons to identify the beneficial owner.

15.18. Upon the identification of a natural person, the obliged entity must also identify the beneficial owner of the natural person, i.e. the person who controls and benefits from the person's activity. Suspicions about the existence of a beneficial owner may arise primarily if, upon the implementation of due diligence measures, the obliged entity feels that the natural person has been influenced to establish the business relationship or conclude the transaction. In such a case, the person who exercises control over the natural person must be considered the beneficial owner of the natural person.

15.19. If the obliged entity ascertains that transactions or actions are actually performed on behalf of a third party, and the content of the activities suggests the possible activities of a trust, the obliged entity must take all measures to identify the beneficial owner of the trust and perform all actions to ascertain the actual purpose of the business relationship. For the purposes of the General Part of the Civil Code Act, this may mean that a business relationship with such a trust cannot be established, as the person who actually wants to establish the business relationship or perform the act is a trust that does not have legal capacity pursuant to Estonian law.

15.20. The obliged entity shall record and retain information of all operations carried out to identify the beneficial owner.

16. POLITICALLY EXPOSED PERSON AND THEIR IDENTIFICATION

16.1. Upon the establishment of a business relationship and as in the course of a business relationship or if a certain trigger event occurs, the obliged entity will take measures to ascertain whether the customer or the person and the beneficial owner or representative of these persons is a politically exposed person, their family member or close associate, or if the customer has become such a person.

16.2. A politically exposed person means a natural person who performs or has performed prominent public functions and with regard to whom related risks remain. At least the following persons are deemed to perform prominent public functions:

16.2.1. head of State or head of government;

16.2.2. minister, deputy minister or assistant minister;

16.2.3. member of a legislative body;

16.2.4. member of a governing body of a political party;

16.2.5. judge of the highest court of a country;

16.2.6. auditor general or a member of the supervisory board or executive board of a central bank;

16.2.7. ambassador, envoy or chargé d'affaires;

16.2.8. high-ranking officer in the armed forces;

16.2.9. member of an administrative, management or supervisory body of a state-owned enterprise;

16.2.10. director, deputy director and member of a management body of an international organisation;

16.2.11. person in list of Estonian positions whose holders are considered politically exposed persons is established by a regulation of the minister responsible for the field;

16.2.12. person in list of positions, which is established by international organisation accredited in Estonia;

16.2.13. a person who, as per list published by the European Commission, is considered a performer of prominent public functions by a Member State of the European Union, the European Commission or an international organisation accredited on the territory of the European Union is deemed a politically exposed person.

16.3. Regardless of clause 16.2 of this clause, middle-ranking or more junior officials are not considered politically exposed persons.

16.4. In the case of a customer that is a legal entity or the person must be considered a politically exposed person if their representative or beneficial owner is a politically exposed person or a family member or close associate of the politically exposed person. In the case of a state-owned customer that is a legal entity or a person must be considered a politically exposed person if the politically exposed person has a significant and prominent function in the company and the state owns at least 50% of this company. Upon the assessment of such a significant and prominent function, it is necessary to also assess whether the politically exposed person has any (substantial) authorization over the state's assets or funds or policies or activities, whether they have the right to issue licenses or permits, make exceptions, whether they have control or influence over the accounts or funds of the state or the company, etc.

16.5. **Family member** means the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person; a child and their spouse, or a person considered to be equivalent to a spouse, of a politically exposed person; a parent of a politically exposed person.

16.6. A person known to be **close associate** means a natural person who is known to be the beneficial owner or to have joint beneficial ownership of a legal person or a legal arrangement, or any other close business relations, with a politically exposed person; and a natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person;

16.7. Obliged entities must identify close associates and family members of politically exposed persons only if their connection with the executor of substantial functions of public authority is known to the public or if the obliged entity has reason to believe that such a connection exists.

16.8. Where a politically exposed person no longer performs important public functions placed upon them, the obliged entity must at least within 12 months take into account the risks that remain related to the person and apply relevant and risk sensitivity-based measures as long as it is certain that the risks characteristic of politically exposed persons no longer exist in the case of the person.

16.9. In addition to the relevant due diligence measures, the obliged entity applies inter alia the following additional measures to politically exposed persons:

16.9.1. verifying data or making inquiries in relevant databases or public databases or making inquiries or verifying data on the websites of the relevant supervisory authorities or institutions of the country in which the customer or person is located. Politically exposed persons must be additionally verified using Google and the local search engine of the customer's country of origin, if any, by entering the customer's name in both Latin and local alphabet with the customer's date of birth.

16.10. In addition to the relevant due diligence measures specified in clause 16.9, the obliged entity applies the following measures to politically exposed persons:

16.10.1. obtains the approval from the senior management to establish or continue a business relationship with the person;

16.10.2. applies enhanced due diligence measures in accordance with 7th chapter of this guidelines;

16.10.3. applies additional due diligence measures in accordance with 8th chapter of this guidelines.

16.11. Senior management within the meaning of clause 16.10.1 is the person who has a sufficiently high position, the right to make decisions and thorough knowledge of the organization and its capacity in order to make informed decisions in issues directly affecting the obliged entity's risk profile and who knows that the compensation mechanisms of the obliged entity are adequate for taking such risk.

16.12. The obliged entity shall record and retain information of all operations carried out to identify the politically exposed person.

17. IDENTIFICATION OF SOURCE AND/OR ORIGIN OF WEALTH

17.1. The obliged entity collects information about the source and/or origin of the customer's wealth:

17.1.1. upon the establishment of a business relationship, if appropriate, to identify the purpose and nature of the business relationship;

17.1.2. upon the conclusion of an occasional transaction outside of a business relationship, if appropriate, to identify the purpose and nature of the business relationship;

17.1.3. the obliged entity knows or suspects that the customer or the person concluding an occasional transaction is a politically exposed person, their family member or close associate.

17.2. Establishment of the source and/or origin of wealth means that the obliged entity identifies a bigger and more general picture of the customer's wealth, i.e. the source of all assets. This usually indicates how many funds the customer may have at all and where the customer received these funds from. In addition to requesting the relevant information from the customer, it may also be possible to collect such information from public databases and other public or non-public data, such as the land register, registers of other assets, declarations of economic interests, registers of companies, etc. The data of the source and/or origin of wealth must be verified on the basis of reliable and independent data, documents and information if the risk associated with the customer is particularly high. The obliged entity should not settle for the general answers of the customer or make unjustified assumptions (e.g. that employees with significant functions have bigger salaries and more assets etc.) and the obliged entity must be convinced that they know the source and/or origin of the customer's wealth. If the customer refuses to disclose data about the source and/or origin of their wealth or gives general answers or the data differ from the data that are publicly or non-publicly accessible, this may be a situation that points at a higher risk to which enhanced attention must be given, i.e. with regard to which enhanced measures must be taken.

18. DUE DILIGENCE MEASURES DURING BUSINESS RELATIONSHIP

18.1. The obliged entity must observe the business relationship with the customer established in the course of economic or professional, i.e., perform the monitoring of the business relationship.

18.2. The obliged entity shall implement the following measures as part of the monitoring of the business relationship:

18.2.1. ensuring that the documents, data, or information collected in the course of the application of due diligence measures are updated regularly and in the case of trigger events, i.e., primarily the data concerning the person, their representative (incl. the right of representation) and beneficial owner;

18.2.2. continuous monitoring of the business relationship, which covers transactions carried out in the business relationship to ensure that the transactions correspond to the obliged entity's knowledge of the customer, their risk profile;

18.2.3. identification of the source and origin of funds used in a transaction.

18.3. The obliged entity must regularly check and update the documents, data and information collected in the course of the application of due diligence measures. The regularity of the checks must be based on the risk profile of the customer and the checks must take place at least:

18.3.1. once semi-annually for a high-risk profile customer;

18.3.2. once annually for a medium-risk profile customer;

18.3.3. once every two years for a low-risk profile customer.

18.3.4. The collected documents, data and information must also be checked if an event has occurred which indicates the need to update the collected documents, data and information.

18.4. In the course of the **ongoing monitoring of a business relationship**, the obliged entity must monitor the transactions concluded during the business relationship in such a manner that the latter can determine whether the transactions to be concluded correspond to the information previously known about the customer (i.e., what the customer declared upon the establishment of the business relationship or what has become known in the course of the business relationship). The obliged entity must also monitor the business relationship to ascertain the customer's activities or facts that indicate criminal activities, money laundering or terrorist financing or the relation of which to money laundering or terrorist financing is probable, incl. complicated, high-value and unusual transactions and transaction patterns that do not have any reasonable or obvious economic or legitimate purpose or that are uncharacteristic of the specific features of the business in question. In the course of the business relationship, the obliged entity must constantly assess the changes in the customer's activities and assess whether these changes may increase the risk level associated with the customer and the business relationship, giving rise to the need to apply additional or enhanced due diligence measures.

18.5. In the course of the ongoing monitoring of the business relationship, the obliged entity applies the following measures:

18.5.1. screening i.e., monitoring transactions in real-time;

18.5.2. monitoring i.e., analyzing transactions later;

18.6. The objective of **screening** is to identify:

18.6.1. suspicious and unusual transactions and transaction patterns;

18.6.2. transactions exceeding the provided thresholds;

18.6.3. politically exposed persons and circumstances regarding international sanctions.

19. OUTSOURCING ACTIVITY TO ANOTHER PERSON

19.1. The obliged entity has the right, considering the special requirements and restrictions stipulated in legislation, to use the services of another person on the basis of a contract, the content of which is the continued performance of activities and acts

that are necessary for the provision of the service(s) by obliged entities to customers and that would ordinarily be performed by the obliged entity themselves. Another person within the meaning of this point is, for example, an agent, subcontractor or another person to whom the obliged entity outsources an activity related to the provision of these services, which the obliged entity performs themselves in their economic activities as a rule. The obliged entity outsources an activity in a situation where another person implements the requirements arising from the applicable legislation and/or these guidelines on behalf and for the account of the obliged entity. This obligation differs from relying on another person where the other person implements the requirements arising from the applicable legislation and/or these guidelines for the performance of their obligations arising from law, after which the obliged entity uses them in the performance of their obligations and relies on these data.

19.2. In order to outsource an activity within the meaning of clause 19.1, the obliged entity must implement an outsourcing policy/risk assessment that is approved by the management board of the obliged entity. At least the following must be analyzed, considered, and described in this document:

19.2.1. the impact of outsourcing on the business activities of the obliged entity and the manifesting risks (e.g., operational risk, incl. IT and legal risk, reputation risk and concentration risk);

19.2.2. the reporting and supervision procedure implemented from the start to the end of the outsourcing contract (incl. preparation of the description of outsourcing, entry into the outsourcing contract, performance of the contract until its expiry, situation plans and strategies for termination of the contract);

19.2.3. in the event of outsourcing an internal activity of the consolidation group, the procedure for outsourcing, incl. the services provided by a legal entity belonging to the consolidation group of the obliged entity, and the specific features of the consolidation group;

19.2.4. the procedure and methodology for selecting and assessing the other person.

19.3. The obliged entity may outsource the obligation to fully or partly apply the due diligence measures specified in these guidelines (i.e., the identification of the customer, beneficial owner, politically exposed person, the source and/or origin of wealth and the purpose and nature of the business relationship) only:

19.3.1. to other obliged entity;

19.3.2. to an organization, association or union whose members are obliged entities; or

19.3.3. to another person who applies the due diligence measures and data retention requirements provided for in the applicable legislation and in these guidelines and who is subject to or is prepared to be subject to AML supervision or financial supervision in a contracting state of the European Economic Area regarding compliance with requirements.

19.4. The obligation to apply due diligence measures not specified in clause 19.3 cannot be outsourced. This restriction does not apply to outsourcing activities related to the identification and implementation of international sanctions.

19.5. The obliged entity selects the other person specified in clause 19.1 with due diligence to ensure the capacity of this person to comply with the requirements of the applicable legislation and these guidelines and ensure the reliability and necessary qualification of this person. When outsourcing the activity (activities) of the obliged entity, the obliged entity must ensure that the other person has the required knowledge and skills, primarily for identifying suspicious and unusual situations, and

that they are capable of complying with all of the money laundering and terrorist financing prevention requirements stipulated by legislation. In order to comply with the provisions of this clause, the obliged entity must make sure that the managers of the other entity are informed about the relevant requirements and ensure training of employees about the prevention of money laundering and terrorist financing to a necessary extent.

19.6. To outsource an activity, the obliged entity enters into a written contract with the other person. The contract must ensure:

19.6.1. division of the rights and obligations associated with the outsourcing of the activity, incl. data retention, reporting to the Financial Intelligence Unit(s), etc.;

19.6.2. that the outsourcing of the activity does not impede the activities of the obliged entity or performance of the obligations provided for in the applicable legislation and these guidelines;

19.6.3. that the other person performs all the obligations of the obliged entity relating to the outsourcing of the activity;

19.6.4. that the outsourcing of the activity does not impede exercising supervision over the obliged entity;

19.6.5. that the competent authority can exercise supervision over the person carrying out the outsourced activity via the obliged entity, incl. by way of an on-site inspection or another supervisory measure;

19.6.6. the required level of knowledge and skills and the capacity of the other person and the set of measures taken for this purpose, incl. regular training;

19.6.7. that the obliged entity has the unrestricted right to inspect compliance with the requirements provided for in the RahaPTS and these guidelines;

19.6.8. that documents and data gathered for compliance with the requirements arising from the RahaPTS and these guidelines are retained and, at the request of the obliged entity, copies of documents relating to the identification of a customer and their beneficial owner or copies of other relevant documents are handed over or submitted to the competent authority immediately. The contract must guarantee that any information that is relevant in the course of the application of due diligence measures is handed over to the obliged entity and/or the relevant data and documents are archived pursuant to the procedure set forth in their rules of procedure;

19.6.9. the right of the obliged entity to terminate the outsourcing contract with the other person, where necessary, if the latter has failed to perform the contractual obligations or has not performed them properly.

19.7. The obliged entity immediately informs the competent supervisory authority about entry into the contract that serves as a basis for outsourcing their activity (activities). When providing information, the obliged entity shall indicate, inter alia, the scope of the transferred activity. At the request of the competent supervisory authority, the obliged entity shall provide the contract for the outsourcing of activities.

19.8. The obliged entity is not allowed to outsource activities to an entity that has been established in a high-risk third country.

19.9. All of the money laundering and terrorist financing prevention requirements stipulated by legislation extend to the other person in respect of the outsourced activity (activities) within the meaning of clause 19.1. The obliged entity that has outsourced an activity is responsible for compliance with requirements and therefore also for any violations.

Source: Developed by the author

Appendix 12. Risk tool references (extract)

Country Risk

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
AFGHANISTAN	Prohibited	Prohibited	NO	1. FATF's call for higher risks of the financial system in connection with terrorism and money laundering 2. The second in the rating of the world's AML risk 3. United Nations and EU sanctions	Unwillingness of the state government to participate in meetings of international bodies for combating money laundering and the financing of terrorism. Ban on financial transactions.
ALBANIA	High risk	8	YES	Recently excluded from the FATF list of monitored countries (2015)	
ALGERIA	Medium risk	6.28	YES	1. FATF's call for higher risks of the financial system in connection with terrorism and money laundering	A country with a high level of corruption and money laundering. Illegal income mainly resulting from smuggling of everyday goods, cigarettes, people trafficking, weapons trade and transport, drugs, extortion and kidnapping for ransom. The financial system is built on transactions in cash.
ANDORRA	High risk	8	YES	Tax haven	

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
ANGOLA	Medium risk	6.33	YES	1. FATF's call for higher risks of the financial system in connection with terrorism and money laundering 2. EU sanctions	A very high level of corruption, a transit country for drugs from Brazil and other areas of South America, a high level of smuggling of weapons, diamonds, cars and also presence of human trafficking. The financial system is built mainly on cash.
ANGUILLA	High risk	8	YES	Tax haven	The financial sector is small compared to other jurisdictions in the Caribbean, but the possibility to register companies on the Internet, zero taxation, and the use of bearer shares makes the country vulnerable to money laundering.
ANTIGUA AND BARBUDA	High risk	8	YES	Tax haven	Antigua and Barbuda remains a significant offshore center, which continues to be vulnerable to money laundering and other financial crimes. The increase in drug trafficking, the large financial sector, and the growth of the online gambling industry also

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
					increases the ML risks.
ARGENTINA	Medium risk	6.5	YES		Argentine and international observers are concerned that money laundering in the country is linked to illicit drug trafficking, corruption, smuggling and tax evasion that occurs throughout the whole financial system. The most common money laundering operations in the non-financial sector include operations conducted using of lawyers/law companies, accountants, corporate structures and real estate sector. The widespread use of cash (including US dollars) in the economy also leaves Argentina vulnerable to money laundering.
ARMENIA	Medium risk	5.08	YES	Sanctions	

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
ARUBA*	High risk	8	YES	Tax haven	Aruba is semi-autonomous part of Netherlands. Because of its location, it is a transit point for the drugs from South America going to the US and Europe, and a staging post for the currency in the opposite direction. Mass contraband of money represents a risk due to the location of Aruba between North and South America. Money laundering is primarily related to the proceeds from the trade in illicit drugs and occurs through the purchase of real estate and tax evasion.
AUSTRALIA	Low risk	3.97	YES		
AUSTRIA	Medium risk	4.64	YES		
AZERBAIJAN	Medium risk	5.31	YES	Sanctions	

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
BAHAMAS	High risk	8	YES	tax haven, drug trafficking, high level of money laundering	The Bahamas remain a staging post for the transit of illegal drugs. The main sources of laundered proceeds is the transit of drugs and weapons and illegal gambling. There is a significant black market of contraband cigarettes and weapons. Money laundering schemes include the purchase of real estate, large capacity vehicles, boats and jewelry, and the processing of money through a complex network of legitimate enterprises and international companies registered in the offshore area of the financial sector. Drug dealers and other criminal organizations use a large number of offshore banks registered in the Bahamas to launder large sums of money, despite the stringent AML requirements of the local banks.

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
BAHRAIN	Medium risk	5.46	YES	Tax haven	Bahrain is the leading financial center in the Persian Gulf region. The greatest risk of money laundering stems from illicit proceeds of foreign origin. The extensive network of the Bahrain banking system, along with its geographical location in the Middle East as a transit point on the Gulf Coast and in South-West Asia, makes it attractive for money laundering activities. Bahrain does not have a significant black market for smuggled goods or known links to illicit drug trafficking.
BANGLADESH	Medium risk	5.8	YES		While Bangladesh is not a regional financial center, its geographical location, seaports and long porous borders with India and Burma have made it a staging post for drugs. Illicit drug trafficking, corruption, fraud, money

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
					counterfeiting and human trafficking are the main sources of illegal/crime proceeds. Bangladesh is also vulnerable to the financing of terrorism, including funding through the hawala / hundi system. While much still needs to be changed, Bangladesh has taken important steps to prevent the use of the financial system to finance terrorism.
BARBADOS	Prohibited	9	NO	Tax haven	Money laundering takes place in Benin through the banking system and other MSRP. In particular, proceeds from the drug trade are known to be combined with the sale of imported second-hand cars sold primarily in neighboring countries. From 2007 to 2013, Benin was used in major international schemes in which Lebanese financial institutions (including one connected with Hezbollah) were used to launder and

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
					move criminal proceeds through West Africa. Under the scheme, funds were spent from Lebanon to the United States to buy used cars, which were then sent to Benin and sold throughout West Africa. The profits from the sale of these cars were combined with drug revenues from Europe, and then shipped to Lebanon. Hezbollah, which the US State Department has recognized as a foreign terrorist organization, was funded by this scheme.
BELARUS	Prohibited	9	NO	Multiple Sanctions	
BELGIUM	Medium risk	4.29	YES		
BELIZE	High risk	8	YES	Tax haven	
BENIN	High risk	7.27	YES		
BERMUDA*	High risk	8	YES	Tax haven	Bermuda is one of the main offshore financial centers. This is the third largest reinsurance center in the world. Money laundering occurs in Bermuda, mainly in connection with

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
					domestic drug trafficking. The laundered money is controlled primarily by domestic criminal organizations that have been growing in recent years.
BHUTAN	High risk	8	YES		
BOLIVIA	Medium risk	6.01	YES		One of the three main countries for cocaine transport, human trafficking and terrorism.
BOSNIA AND HERZEGOVINA	Medium risk	5.83	YES	Balkan sanctions	
BOTSWANA	Prohibited	9	NO		a high level of money laundering related to drug trafficking and an increased number of organized groups. The financial system is built on transactions in cash.
BRAZIL	High risk	8	YES		In 2013, Brazil was the seventh largest economy in the world by nominal GDP. This is one of the main countries of drug transit in the world, as well as one of the largest consumer countries in the world. São Paulo, the largest city in Brazil, is

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
					considered the regional financial center of Latin America. Money laundering in Brazil is primarily related to domestic crimes, especially with illicit drug trafficking, corruption, organized crime, gambling and other various types of smuggling. Money laundering channels include the use of banks, real estate investments, financial asset markets, luxury goods and informal financial networks.
BRITISH VIRGIN ISLANDS *	High risk	8	YES	Tax haven	The British Virgin Islands (BVI) is the territory of Great Britain. The economy is highly dependent on tourism and offshore financial sector. The Financial Services Commission (FSC) is the only supervisory authority responsible for licensing and supervising financial institutions under the relevant laws. The proximity to

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
					the US Virgin Islands creates additional risk factors for money laundering. The British Virgin Islands are the main target for drug traffickers who use the area as a gateway to the United States. Illicit drug traffic as a whole is a serious problem.
BRUNEI DARUSSALAM	High risk	8	YES	Tax haven	
BULGARIA	Low risk	3.51	YES		
BURKINA FASO	High risk	8	YES	Limited information is available	High level of corruption and money laundering through smuggling and transit of drugs and products of the black market. An undeveloped financial system - only 6% of the population have bank accounts. Very weak legal system.
BURUNDI	Prohibited	9	YES	Limited information is available	A very high level of corruption, one of the poorest countries in the world (due to a prolonged civil war).

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
CAMBODIA	Prohibited	9	NO	FATF Statement re AML Strategic Deficiencies: 23 October 2020	Cambodia is neither a regional nor an offshore financial center, but several factors contribute to the significant vulnerability of Cambodia's financial system to money laundering. This includes weak and ineffective AML regime, the dollarized economy, the rapid growth of the official banking sector, porous borders, non existent casino supervision, and limited capacity of the National Bank of Cambodia.The weak judicial system and corruption are additional negative factors. Cambodia also has a significant black market of contraband goods, including medicines and imported substances for the local production of methamphetamine. Legitimate and illegal transactions, regardless of size, are often

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
					committed outside formal financial institutions and difficult to control. The proceeds from crime are easily channeled into real estate, luxury goods and other forms of property without going through the official banking sector.
CAMEROON	High risk	8	NO	Cameroon was deemed a 'Monitored' Jurisdiction by the US Department of State 2016 International Narcotics Control Strategy Report (INCSR). Most significant financial crimes in Cameroon derive from domestic public corruption, tax evasion, and embezzlement.	high level of corruption, money laundering and tax evasion. The financial system is built on transactions in cash.
CANADA	Medium risk	4.92	YES		
CABO VERDE	High risk	8	NO	high level of money laundering	Vulnerable to narcotics trafficking between West Africa, the Americas, and Europe. Its financial system is primarily

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
					composed of the banking sector.
CAYMAN ISLANDS *	High risk	8	YES	Tax haven	The Cayman Islands, the territory of the United Kingdom of the Caribbean, is an offshore financial center. Money laundering, first of all, is connected with fraud and drug trafficking. Due to its status as a zero tax regime, the Cayman Islands is also considered attractive to those who seek to evade taxes in their home countries. Gambling is illegal. Cayman Islands do not allow the registration of offshore gaming persons.
CENTRAL AFRICAN REPUBLIC	Prohibited	9	NO	OFAC - Fin. sanctions against all persons associated with the state	An unstable political situation is present along with high level of violence. High level of corruption, the country of transit of smuggling diamonds, weapons and human trafficking.
CHAD	Prohibited	9	YES	Limited information is available	High level of smuggling of cigarettes, food, oil, weapons and drugs (cannabis

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
					and cocaine). Very high levels of corruption, poaching and money laundering.
CHILE	Medium risk	6	YES		
CHINA	Medium risk	6.59	YES	Sanctions	EU sanctions on the arms trade. The main sources of criminal proceeds include corruption, drugs and human trafficking, smuggling, economic crimes, theft of intellectual property, counterfeit goods, crimes against property and tax evasion. Chinese officials noted that corruption in China often includes state-owned enterprises, including in the financial sector. Money-laundering, as a rule, includes: trade on the basis of money laundering; manipulation of bills for services and shipment of goods; purchase of valuable assets, such as real estate; investment of illegal funds in legal sectors; gambling; and the exploitation of

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
					official and underground financial systems.
COLOMBIA	Medium risk	5.83	YES	1. Production of drugs 2. high level of money laundering	
COMOROS	High risk	7	YES		
COOK ISLANDS	High risk	8	YES	Tax haven	The Cook Islands is not a regional financial center and does not have free trade zones. The substantial offshore financial sector of the Islands is an important part of the country's economy, but also represents an increased risk in relation to money laundering and the financing of terrorism. The Government of the Cook Islands is taking measures to reduce risks. There are no data on the level of corruption.
COSTA RICA	Medium risk	5.23	YES	Tax haven	A very high level of corruption and money laundering

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
					through the organization of gambling, human trafficking, smuggling and transit of drugs.
CROATIA	Low risk	3.82	YES	Balkan sanctions	
CUBA	High risk	8	YES	US sanctions	The geographical position of Cuba between the countries that supply and consume drugs poses problems for the authorities. Cuba has little foreign investment, an insignificant presence of international business, there are no offshore casinos or online gaming sites. Since 1963, the US Government has imposed restrictions on travel and money transfers to Cuba and prohibits the import of most Cuban-origin products and, with some exceptions, the export of goods from the United States to Cuba. In addition, the number of US-based assets of the Government of Cuba or Cuban citizens are frozen.

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
CURACAO	High risk	8	YES	Tax haven	
CYPRUS	Medium risk	5.01	YES	Tax haven	
CZECH REPUBLIC	Medium risk	4.15	YES		
DEMOCRATIC REPUBLIC OF THE CONGO	Prohibited	Prohibited	NO	1. OFAC - fin. sanctions against all persons associated with the state 2. A large number of international sanctions	
DENMARK	Low risk	3.95	YES		
DJIBOUTI	High risk	8	NO	Tax haven	Djibouti is one of the most stable countries in the region of Africa. This is a small financial center in the region, thanks to its dollar peg to the US currency and the absence of currency controls. Djibouti's GDP continues to grow by more than four percent a year due to a sharp increase in foreign capital inflows - primarily from the countries of the Gulf Cooperation Council and China - in the maritime, construction and tourism sectors. Smuggled goods consist mainly of taxable cigarettes and alcohol.

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
DOMINICA	High risk	8	YES	Tax haven	The Dominican Republic (DR) is not a major regional financial center, despite the fact that it is one of the largest economic centers in the Caribbean. It continues to be the main transit point for transshipment of illicit drugs destined for the United States and Europe. Corruption in the government and the private sector, the presence of international cartels with illicit trafficking, a large informal sector of the economy, and the fragile sector of the official economy make the Dominican vulnerable to money laundering and terrorist financing. A large informal economy is a significant market for illicit or smuggled goods.
DOMINICAN REPUBLIC	High risk	7	YES	transit of drugs	
EAST TIMOR (Timor Leste)	High risk	7	YES		

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
ECUADOR	Prohibited	9	NO	FATF Call for High Risk	One of the main countries for the transit of drugs, a high level of corruption and money laundering.
EGYPT	High risk	8	YES	Sanctions	Medium to high level of corruption, high level of money laundering and tax evasion. Sanctions are aimed only at former President Mubarak and individuals associated with him. Unstable political situation.
EL SALVADOR	High risk	8	YES	Lack of compliance with Egmont Group principles relating to operational independence and autonomy.	The transit country for South African cocaine. The drug trade is also closely related to the arms trade. High level of corruption, money laundering and financial fraud.
EQUATORIAL GUINEA	Prohibited	9	NO	No information is available	Equatorial Guinea is not a regional financial center. The oil-rich country has a very low level of health and education. The implementation of its AML legislation is not complete and ensuring the weak. The greatest concern in terms of money laundering and terrorist financing is currency

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
					transactions and illegal international money transfers by companies or corrupt individuals.
ERITREA	Prohibited	Prohibited	NO	1. OFAC - fin. sanctions against all persons associated with the state 2. A large number of international sanctions	The country of transit of smuggling, human trafficking and forced sexual slavery
ESTONIA	Low risk	2.68	YES		
ETHIOPIA	Prohibited	Prohibited	NO	sanctions were applied in the past, one of the poorest countries.	A high level of corruption and money laundering through the organization of gambling, human trafficking and weapons, smuggling and transit of drugs. One of the poorest countries in the world.
FIJI	Prohibited	9	NO	EU Tax Blacklist	Sanctions against the family of government and arms trade established by the EU, Australia and New Zealand. Politically unstable state, highly military. There is no information on the level of corruption.
FINLAND	Low risk	3.17	YES		

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
FRANCE	Medium risk	4.09	YES		
French Guinea	Prohibited	9	NO		
GABON	Prohibited	9	NO	Limited information is available	
GAMBIA	Medium risk	6.5	YES	Limited information is available	The country of transit of marijuana and cocaine. high level of corruption and money laundering.
GEORGIA	Medium risk	5.2	YES		
GERMANY	Medium risk	4.49	YES		
GHANA	High risk	8	YES	FATF AML Deficient List	
GIBRALTAR*	High risk	8	YES	Tax haven	
GREECE	Medium risk	4.56	YES		
GRENADA	High risk	7	YES	Tax haven	The geographical location of Grenada places it in close proximity to drug trafficking routes from South America to the United States and Europe. This is not a regional financial center. As a transit point, money laundering in Grenada is mainly related to the smuggling and trafficking of drugs by local crime groups. Illegal income is usually laundered through various businesses, as well as by

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
					purchasing real estate, boats, jewelry and cars.
Guadeloupe	High risk	8	YES		
GUATEMALA	High risk	8	YES	Tax haven	The transit country of South African cocaine and heroin and the smuggling of synthetic drugs. The drug trade is so closely related to the arms trade. high level of corruption and money laundering.
GUERNSEY*	High risk	8	YES	Tax haven	
GUINEA	Prohibited	Prohibited	NO	1. OFAC - fin. sanctions against all persons associated with the state 2. A large number of international sanctions	Sanctions against the trade, transit and export of weapons and equipment that can be used for internal repression due to the high level of corruption and financial system based on cash. The country of transit of drugs and smuggling of cars, diamonds and gold.
GUINEA-BISSAU	Prohibited	Prohibited	NO	1. 5th place in the rating of the world AML Risk 2. Sanctioned by the United Nations and EU	EU sanctions on financial resources. The country of transit of drugs, a very high level of corruption, one of the poorest

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
					countries in the world.
GUYANA	Medium risk	6.14			
HAITI	High risk	7.34	NO	1. OFAC - fin. sanctions against all persons associated with the state 2. A large number of sanctions related to the state	Absence of strict laws on combating money laundering and corruption
HONDURAS	High risk	7	YES	country of transit and production of drugs.	The country of transit of "dirty" money, high level of corruption and money laundering, which are obtained through the transit of cocaine and human trafficking. The financial system is based mainly illegal funds.
HONG KONG	Medium risk	5.11	YES	Tax haven	
HUNGARY	Medium risk	4.9	YES		
ICELAND	Medium risk	4.66	YES		
INDIA	Medium risk	5.6	YES		
INDONESIA	Medium risk	5.13	NO	FATF Call for High Risk AML	
IRAN	Prohibited	Prohibited	NO	1. The FATF's appeal for the protection of the financial system in connection with terrorism and money laundering state.	Ban on financial transactions.

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
				3. High World AML rating	
IRAQ	Prohibited	Prohibited	NO	1. The FATF's appeal for the protection of the financial system in connection with terrorism and money laundering 2. OFAC - Fin. sanctions against all persons associated with the state. 3. 6th highest AML risk rating in the world	The ban on financial transactions, one of the highest levels of corruption in the world.
IRELAND	Medium risk	4.55	YES		
ISLE OF MAN	High risk	8	YES	Tax haven	
ISRAEL	Low risk	3.76	YES		
ITALY	Medium risk	4.99	YES		
IVORY COAST	Prohibited	Prohibited	NO	1. OFAC - fin. sanctions against all persons associated with the state 2. A large number of international sanctions	
JAMAICA	Medium risk	6.24	YES	Tax haven	The country has a very high level of money laundering, obtained through the sale of illegal drugs and financial fraud by organized criminal groups.
JAPAN	Medium risk	5.02	YES		
JERSEY	High risk	8	YES	Tax haven	

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
JORDAN	Medium risk	4.77	YES	Tax haven	The Jordan has a well-developed financial sector with significant banking relations in the Middle East. Long and remote borders of the Jordan desert and proximity to Iraq, Syria, Saudi Arabia and Israel make it susceptible to smuggling of gold, oil, drugs, cigarettes, counterfeit goods and other contraband. Money laundering incidents are rare, and recent incidents include individual foreign and Jordanian persons laundering by holding positions in government agencies or public companies.
KAZAKHSTAN	Medium risk	6.27	YES		
KENYA	High risk	7.33	YES	13th highest AML risk rating in the world	A very high level of corruption and money laundering through drug transit, a smuggling point for most African countries and poaching.
KIRIBATI	Prohibited	9	NO		A weakly developed country, no information on the level of

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
					corruption, compliance issues with the world standards of the financial market and the fight against money laundering and the financing of terrorism.
KOSOVO	High risk	8	YES	Balkan sanctions	
KUWAIT	Prohibited	9	NO	tax haven, recently (2015) excluded from the monitoring list of the FATF	Financial crimes, such as money laundering, and financial support for terrorist groups, on the part of individuals who work outside of government-approved charities, raise serious suspicions.
KYRGYZSTAN	High risk	7	YES		The big shadow economy, corruption, organized crime and drug business make the country vulnerable to financial crimes. Although there is no official data, it is known that drug trafficking is the main source of income from criminal activity, since the Kyrgyz Republic is located on the territory of the "northern transit route" passing from

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
					Afghanistan to the Russian Federation along the key. In addition, smuggling of consumer goods, including fuel, and corruption among officials continues to be the main source of criminal proceeds. Weak political system, resource constraints, ineffective financial system and corruption suppress efforts to effectively combat money laundering.
LAO PDR	Prohibited	10	NO	The FATF call for a high-risk due to Aml Risk	Very high levels of corruption, drug sale and money laundering.
LATVIA	Medium risk	4.89	YES		
LEBANON	Prohibited	Prohibited	NO	1. OFAC - fin. Sanctions against persons associated with the state 2. A large number of international sanctions 3. Tax haven	Sanctions against the country to ban financial transactions.
LESOTHO	High risk	8	YES		
LIBERIA	High risk	8	YES	1. High AML risk rating in the World (16) 2. A large number of sanctions	The lack of regulation of the gambling market and the low level of regulation of the financial market contribute to an increased risk of

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
					money laundering and terrorist financing.
LIBYA	Prohibited	Prohibited	NO	1. OFAC - fin. sanctions against all persons associated with the state 2. A large number of international sanctions	The country is a transit country for drugs and smuggling from Africa and China. Because of the revolution in 2011, the state is unstable economically and politically - the armed forces are involved in criminal activities, such as extortion and illegal arms sales.
LIECHTENSTEIN	High risk	7	YES	Tax haven	
LITHUANIA	Low risk	3.55	YES		
LUXEMBOURG	Medium risk	4.82	YES		
MACAO	High risk	8	YES	Tax haven	A country with a high turnover of funds from gambling, which is associated with money laundering and fraud. There is no information on the level of corruption.
MACEDONIA	Low risk	3.22	YES		
MADAGASCAR	High risk	7	YES		
MALAWI	High risk	7	YES		
MALAYSIA	Medium risk	6.5	YES		

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
MALDIVES	High risk	8	YES	Tax haven	The Maldives consist of a number of atolls in the Indian Ocean and are separated by a number of international sea lanes, and the authorities have expressed concern that the islands are currently being used as a transit point for money laundering and illegal immigration to Europe.The country has a small financial market, but it is susceptible to money laundering and the financing of terrorism due to limited surveillance capabilities. Official data are not available, but according to unofficial data, illegal drug trafficking, a large black market for dollar trading and corruption constitute a significant part of the amount of illegal funds.
MALI	Prohibited	Prohibited	NO	7th highest AML risk rating in the world	
MALTA	Medium risk	5.38	YES	Tax haven	

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
MARSHALL ISLANDS	High risk	8	YES	Tax haven	Domestic non-resident corporations (NRDCs), the equivalent of international companies, can be registered on the Internet. Such companies have the right to offer bearer shares, the corporate officers, directors and shareholders can be of any nationality and live in any jurisdiction. NRDCs are not required to disclose the names of officials, directors, shareholders, or beneficial owners specified in the Register, and legal entities may act as directors, officers and shareholders. These factors constitute the overall high ML risk of the Islands.
Martinique (France, Antilly)	High risk	8	YES		
MAURITANIA	Prohibited	9	NO		High level of corruption and money laundering through smuggling and transit of drugs. An undeveloped financial system - only 4% of the

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
					population have bank accounts.
MAURITIUS	High risk	8	YES	Tax haven	
MEXICO	Medium risk	5.13	YES	1. Production of drugs 2. high level of ML	
MICRONESIA	Prohibited	9	NO		
MOLDOVA	High risk	8	YES	Sanctions	
MONACO (FRANCE)	High risk	8	YES	Tax haven	
MONGOLIA	Medium risk	6.57	YES		
MONTENEGRO	Low risk	3.94	YES	Balkan sanctions	
MONTSERRAT* (Antilly)	High risk	8	YES	Tax haven	
MOROCCO	High risk	8	YES		
MOZAMBIQUE	High risk	8.22	NO	9th highest AML risk in the world	The transit country of drugs, which is closely related to the arms trade. High level of corruption, money laundering and financial fraud.
MYANMAR	Prohibited	Prohibited	NO	1. FATF's call for higher risks of the financial system in connection with terrorism and money laundering 2. OFAC - Fin. sanctions against all persons associated	Very slow progress in improving the country's legislation in relation to the fight against money laundering and the financing of terrorism. A high level of corruption,

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
				with the state. 3 10th highest AML risk rating in the world 4. European sanctions, US sanctions	a transit country for drugs.
NAMIBIA	Prohibited	10	NO	Recently excluded from the list of monitored countries of FATF (2015), narcotransit	
NAURU	High risk	8	YES	Tax haven	
NEPAL	Prohibited	10	NO	14th highest AML risk rating in the world	
NETHERLANDS	Medium risk	4.86	YES		
NETHERLANDS ANTILLES*	High risk	8	YES	Tax haven	
NEW ZEALAND	Low risk	3.18	YES		
NICARAGUA	Prohibited	Prohibited	NO	Recently excluded from the monitoring list of FATF (2015), narcotransit	High level of corruption and money laundering through smuggling, drug trafficking and trafficking.
NIGER	Prohibited	10	NO	limited information is available, one of the poorest countries in the world	Weak legislation to combat money laundering. INCSR (International Drug Trafficking Control Service) monitors the country. One of the poorest and least developed countries in the world. High level

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
					of money laundering and financial crimes. Country of transit of drugs.
NIGERIA	High risk	8	NO	UN sanctions. Laundering of money	One of the main countries for the transit of drugs, a high level of corruption, money laundering and various types of fraud.
NIUE	High risk	8	YES	Tax haven	
NORTH KOREA	Prohibited	Prohibited	NO	1. OFAC - fin. sanctions against all persons associated with the state 2. A large number of international sanctions	Sanctions against the country for financial transactions. Unwillingness of the government of the state to go to the meeting to the bodies for combating money laundering and financing of terrorism.
NORWAY	Low risk	3.91	YES		
OMAN	Medium risk	5	YES		
PAKISTAN	Prohibited	9	NO	FATF AML Deficient List. Recently excluded from the FATF list (2015), high level of money laundering, narcotransit	The country of transit of drugs and smuggling from Afghanistan. Very high levels of corruption, tax evasion, human trafficking and terrorism.
PALAU	Prohibited	9	NO	Limited information is available	The high level of corruption associated with trafficking in

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
					illegal drugs and prostitution.
PALESTINE*	High risk	8	YES		High level of corruption, the territory of drug transit, US and Israeli sanctions against financial transactions. Unstable political situation.
PANAMA	Prohibited	9	NO	FATF AML Deficient List. The FATF call for a high-risk due to Aml Risk	High level of corruption and money laundering through smuggling, drug transit, tax evasion and human trafficking. Very weak financial and legal systems.
PAPUA NEW GUINEA	Prohibited	10	NO	The FATF call for a high-risk due to Aml Risk	
PARAGUAY	Medium risk	6.74	YES	One of the highest ML risk rating in the world (15), high level of ML	
PERU	High risk	8	YES	drug transit country	High risks associated with drug trafficking. According to the latest US government statistics, Peru is the world's most important potential producer of cocaine and its exports. High risk of money laundering. High level of corruption. Develops a black market of pirated and contraband goods.

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
PHILIPPINES	Medium risk	5.81	YES		
POLAND	Medium risk	4.34	YES		
PORTUGAL	Medium risk	4.1	YES		
PUERTO RICO	High risk	8	YES	Not on EU White list equivalent jurisdictions	
QATAR	Medium risk	4.97	YES	Tax haven	
REPUBLIC OF THE CONGO	Prohibited	Prohibited	NO	1. OFAC - fin. sanctions against all persons associated with the state 2. A large number of international sanctions	Very slow progress on improving legislation in relation to the fight against money laundering and the financing of terrorism. A high level of corruption, an informal economy based on cash, smuggling weapons, gold, diamonds.
Reunion	Prohibited	9	NO		
ROMANIA	Medium risk	4.76	YES		
RUSSIA	High risk	8	YES	1. OFAC Sanction, EU sanctions, enhanced monitoring	
RWANDA	Prohibited	10	NO	UN sanctions. Rwandan Genocide	Weak legislation to combat money laundering. INCSR monitors the country. There is contraband of tin, tantalum, tungsten and gold from the neighboring Democratic Republic of the Congo. Unstable political situation.

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
SAMOA	High risk	8	YES	Tax haven	
SAN MARINO	High risk	7	YES	Not on EU White list equivalent jurisdictions, Tax haven	A weakly developed country, there is no information on the level of corruption and compliance with the world financial market standards. Average compliance with the standards of anti-money laundering and terrorist financing agencies
SAO TOME AND PRINCIPE	High risk	8	YES	Tax haven	
SAUDI ARABIA	Medium risk	5.26	YES		
SENEGAL	High risk	7	YES		
SERBIA	Medium risk	6.33	YES	FATF 23022018 (EU Balkan sanctions)	
SEYCHELLES	High risk	8	YES	Tax haven	
SIERRA LEONE	High risk	7.2	YES	European and UN sanctions	High level of corruption, smuggling of pharmaceuticals, food, gold, diamonds, money laundering and terrorism.
SINGAPORE	Medium risk	4.58	YES		
SLOVAKIA	Medium risk	4.04	YES		
SLOVENIA	Low risk	3.7	YES		

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
SOLOMON ISLANDS	High risk	8	YES	Limited information is available	The high level of corruption associated with extortion, smuggling and criminal organizations ..
SOMALIA	Prohibited	Prohibited	NO	1. OFAC - fin. sanctions against all persons associated with the state 2. A large number of international sanctions	Unwillingness of the government of the state to go to the meeting to the bodies for combating money laundering and financing of terrorism. The highest level of corruption in the world.
SOUTH AFRICA	Medium risk	4.83	YES		
SOUTH KOREA	Medium risk	4.6	YES		
SOUTH SUDAN	Prohibited	Prohibited	NO	EU and UN sanctions	
SPAIN	Medium risk	4.42	YES	High ML risk	
SRI LANKA	Prohibited	Prohibited	NO		
ST. KITTS & NEVIS	High risk	8	YES	Tax haven	
ST. LUCIA	High risk	8	YES	Tax haven	
ST. VINCENT AND THE GRENADINES	High risk	8	YES	Tax haven	
SUDAN	Prohibited	Prohibited	NO	1. Monitored by FATF as high risk of the Financial System in Connection with Terrorism and	Unwillingness of the government to participate witn int. bodies for combating money

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
				Money Laundering 2. OFAC - Fin. sanctions against persons associated with the state. 3. 12th highest ML risk rating in the world	laundering and the financing of terrorism. The United States recognized the Sudan as the main sponsor of terrorism in the world.
SURINAME	Prohibited	10	NO	EU sanctions	Money laundering in Suriname is closely linked to transnational criminal activities related to the transit of cocaine, primarily to Europe and Africa. There is a smuggling of goods into the country through Guyana and French Guiana.
SWAZILAND	Prohibited	10	NO	8th highest ML risk rating in the world	High level of corruption, money laundering, human trafficking, marijuana and smuggling of cigarettes and alcohol.
SWEDEN	Low risk	3.51	YES		
SWITZERLAND	Medium risk	4.96	YES	High ML risk, tax evasion risk	
SYRIA	Prohibited	Prohibited	NO	1. FATF monitoring on the Higher Risks of the Financial System in Connection with Terrorism and Money Laundering 2. OFAC - Fin. sanctions	Sanctions against financial transactions. High level of corruption. Syria is recognized as the main sponsor of terrorism in the world and one of the main countries

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
				3. International sanctions	for money laundering.
TAIWAN * (China)	Medium risk	5	YES		
TAJIKISTAN	Medium risk	6.28	NO	4th highest ML risk rating in the world	
TANZANIA	Medium risk	6.63	YES		
THAILAND	Medium risk	6.22	YES		
TOGO	Prohibited	9	YES		High level of corruption, human trafficking, high risks associated with drug trafficking, smuggling and money laundering.
TONGA	High risk	8	YES	Tax haven	
TRINIDAD AND TOBAGO	High risk	7	NO	FATF 23022018	
TUNISIA	Prohibited	Prohibited	NO	FATF 23022018	EU sanctions on financial resources. A high risk country for money laundering related to drug transit, corruption, smuggling and illegal immigration.
TURKEY	Medium risk	6.19	YES		
TURKMENISTAN	Prohibited	9	NO	Limited information is available	
TURKS & CAICOS ISLANDS *	High risk	8	YES	Tax haven	

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
TUVALU	Prohibited	9	NO	no AML standards	A weakly developed country, no information on the level of corruption, compliance with the world standards of the financial market and the fight against money laundering and the financing of terrorism.
UGANDA	Prohibited	10	NO	1. The FATF's appeal for the protection of the financial system in connection with terrorism and money laundering, excluded recently on 03.11.2017 2. 11th highest ML risk rating in the world	The financial system is built on cash transactions, which is associated with a high risk of money laundering, terrorist financing and fraud. The financial system is unregulated and unstable.
UKRAINE	High risk	8	YES	1. OFAC Sanctions, EU sanctions, enhanced monitoring	
UNITED ARAB EMIRATES	Medium risk	5.6	YES	Tax haven	
UNITED KINGDOM	Medium risk	4.6	YES	Tax haven	
URUGUAY	Medium risk	6.19	YES	Tax haven	
US VIRGIN ISLANDS *	Prohibited	Prohibited	NO	tax haven, USA	US territory - FATCA.
USA	High risk	7	YES	FATCA, Not on EU White list equivalent jurisdictions	FATCA.

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
UZBEKISTAN	High risk	8	YES		
VANUATU	Prohibited	10	NO	Tax haven	Zone of low taxation and increased risk of money laundering. The economy is based on tourism and agriculture - recent improvements.
VENEZUELA	Prohibited	Prohibited	NO	1. OFAC Sanctions 2. High traffic of cocaine	The country has the highest volume of cocaine transit. Low level of economic development.
VIETNAM	High risk	7.3	YES		
WESTERN SAHARA	Prohibited	9	NO	Limited information is available	
YEMEN	Prohibited	Prohibited	NO	1. FATF monitoring on the Higher Risks of the Financial System in Connection with Terrorism and Money Laundering 2. OFAC - Fin. sanctions 3. Highe ML risk rating rank in the world (17)	Very slow progress in improving the country's legislation in relation to the fight against money laundering and the financing of terrorism. A very high level of state corruption and money laundering due to black market.
ZAMBIA	Prohibited	9	NO	No information is available	Weak financial system, susceptible to use for money laundering, obtained through drug trafficking and human trafficking.

Country	Risk Rate	Risk Rate score (1-10)	Are we cooperating?	Reason for ML risk rating (short)	Description of the ML/TF risks of the country
ZIMBABWE	Prohibited	Prohibited	NO	1. OFAC - fin. Sanctions against persons associated with the state 2. A large number of international sanctions 3. Recent exclusions from the FATF list (2015)	Sanctions against the country and restrictions on the movement of political persons and individual legal entities due to human rights violations and the undermining of democratic processes in the country. A very high level of corruption and money laundering due to smuggling of diamonds.

Type risk

Type	Risk	Risk rating (1-10)
Community interest company.	Medium risk	6
Join-stock private company	High risk	7
Listed company - EEA or equivalent	Low risk	1
Listed company - outside EEA or equivalent	Medium risk	6
Partnership	High risk	8
Private company limited by shares (Ltd.)	High risk	8
Special purpose vehicle (SPV)	Very high risk	9

Relationship risk

Relationship duration	Risk	Risk rating (1-10)
New Client, payment by card	High Risk	10
New Client, payment by bank account	High Risk	8
New Client, payment by bank account (EU, UK and/or EEA to 50 banks)	Medium risk	6
Existing Client 1-3 years	Medium risk	5
Existing Client 3+ years	Low risk	1

Industry risk

Industry	Risk	Risk rating (1-10)
Advisory services	Medium risk	6
Aerospace	Medium risk	5
Agriculture	Medium risk	5
Arms	Very high risk	9
Automotive	Medium risk	6
Broadcasting	Medium risk	5
Chemical	Medium risk	6
Construction	Medium risk	6
Data exchange services	High risk	7
Defense	High risk	7
Education	Low risk	4
Electronics	Medium risk	6
Energy	Medium risk	6
Entertainment	Medium risk	5
Escort services - dating	Very high risk	9
Financial services - crypto - not regulated	Very high risk	9
Financial services - crypto - regulated	High risk	7
Financial services - not regulated	High risk	8
Financial services - payment aggregators	Very high risk	9
Financial services - regulated	Low risk	3
Fishing	Medium risk	6
Food	Medium risk	6
Gambling	Very high risk	9
Health care	Medium risk	6
Hospitality	Medium risk	5
Information	Medium risk	5
Insurance	Low risk	1
Manufacturing	Low risk	2
Marketing	Medium risk	6
Mass media	Medium risk	5
Mediation - car, water, air transport trade	High risk	8
Mining	High risk	7
News media	Medium risk	5
Petroleum	High risk	7
Pharmaceutical	Medium risk	5
Publishing	Medium risk	5
Pulp and paper	Medium risk	5
Real estate	High risk	8
Self Employed	Medium risk	5
Shipbuilding	Medium risk	5
Software	Medium risk	5

Industry	Risk	Risk rating (1-10)
Steel	Medium risk	5
Telecommunications	Medium risk	5
Timber	Medium risk	5
Tobacco	Medium risk	5
Trade - electronics (export-import)	High risk	8
Trade - medicines	High risk	8
Trade - Precious metals	Very high risk	9
Trade - used cars, spare parts	High risk	8
Transportation and logistics	Medium risk	5
Travel agencies	High risk	7
Water	Low risk	3
Wholesale	High risk	7

Product risk

Product	Risk	Risk rating (1-10)
Fiat only	Medium risk	5
Fiat and Crypto exchange	Medium risk	5
Fiat and Crypto transactions	High risk	10
Crypto only	High risk	9
Fiat and Crypto (Limited)	High risk	7

Delivery channel risk

Type	Risk	Risk rating (1-10)
Distant identification	High risk	10
Distant selfie identification	High risk	8
Distant video record identification	Medium risk	7
Distant selfie identification+mashine verification	Medium risk	6
Notary identification	Medium risk	5
Distant video record identification+mashine verification	Low risk	4
Face to face	Low risk	1

Source: LEIpapa OÜ

Appendix 13. The sample output result of the risk rating tool

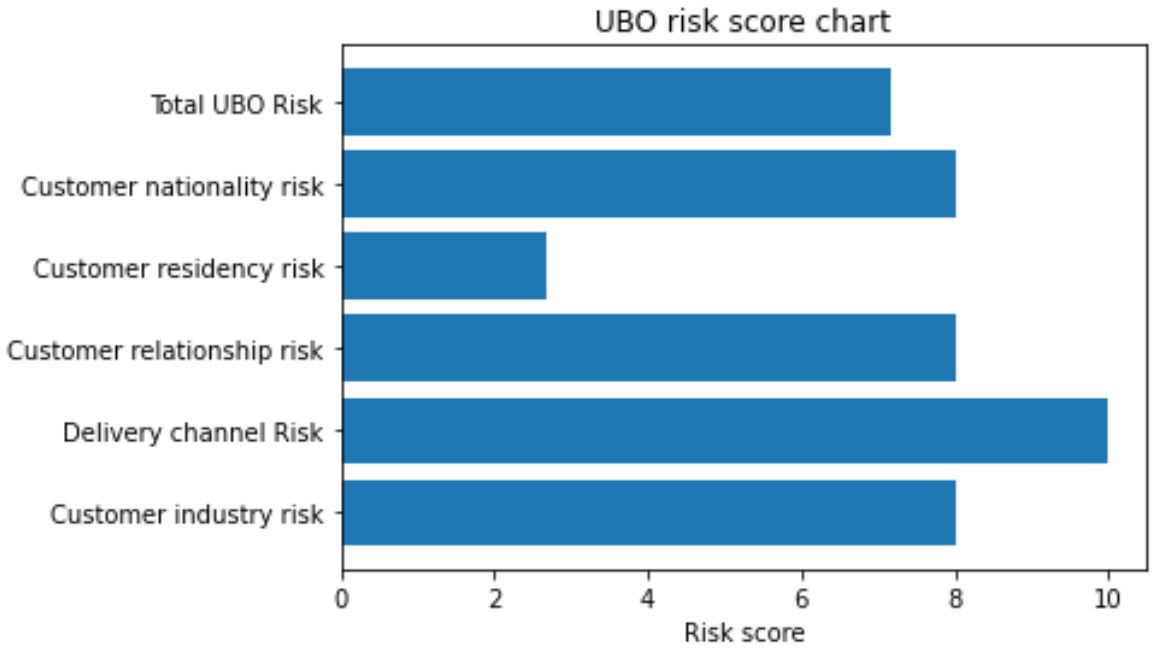
```
LEIPAPA AML TEST SYSTEM VERSION 0.4 NEW RISK TOOL

UBO AML TEST

Enter UBO Name:
Makhmud Makhmudov
Enter UBO ID or Passport number:
BE23546
UBO AML TEST Makhmud Makhmudov BE23546

Choose UBO work industry:
1. Advisory services
2. Aerospace
3. Agriculture
4. Arms
5. Automotive
6. Broadcasting
7. Chemical
8. Construction
9. Data exchange services
10. Defense
11. Education
12. Electronics
13. Energy
14. Entertainment
15. Escort services - dating
16. Financial services - crypto - not regulated
17. Financial services - crypto - regulated
18. Financial services - not regulated
19. Financial services - payment aggregators
20. Financial services - regulated
21. Fishing
22. Food
23. Gambling
24. Health care
25. Hospitality
26. Information
27. Insurance
28. Manufacturing
26. Marketing
27. Mass media
28. Mediation - car, water, air transport trade
29. Mining
30. News media
```

```
31. Petroleum
32. Pharmaceutical
33. Publishing
34. Pulp and paper
35. Real estate
36. Self Employed
37. Shipbuilding
38. Software
39. Steel
40. Telecommunications
41. Timber
42. Tobacco
43. Trade - electronics (export-import)
44. Trade - medicines
45. Trade - Precious metals
46. Trade - used cars, spare parts
47. Transportation and logistics
48. Travel agencies
49. Water
50. Wholesale
Enter work industry type: 18
Industry risk: 8
UBO delivery risk
 1. Distant identification
 2. Distant selfie identification
 3. Distant video record identification
 4. Distant selfie identification+mashine verification
 5. Notary identification
 6. Distant video record identification+mashine verification
 7. Face to face
Enter delivery channel type: 1
Company type risk: 10
UBO relationship risk
 1. New client, no previous bank account
 2. New client, previous bank account
 3. New client, previous bank account (UK and/ot EEA to 50 banks)
 4. Client 1-3 years
 5. Client 3+ years
Enter customer relationship type: 2
Relationship risk: 8
Enter UBO country residency: ESTONIA
ESTONIA Country residence risk: 2.68
Enter UBO country nationality: RUSSIA
RUSSIA Country residence risk: 8
Press "Y" if the UBO is PEP?: Y
Total UBO Risk: 7.17 High risk
```



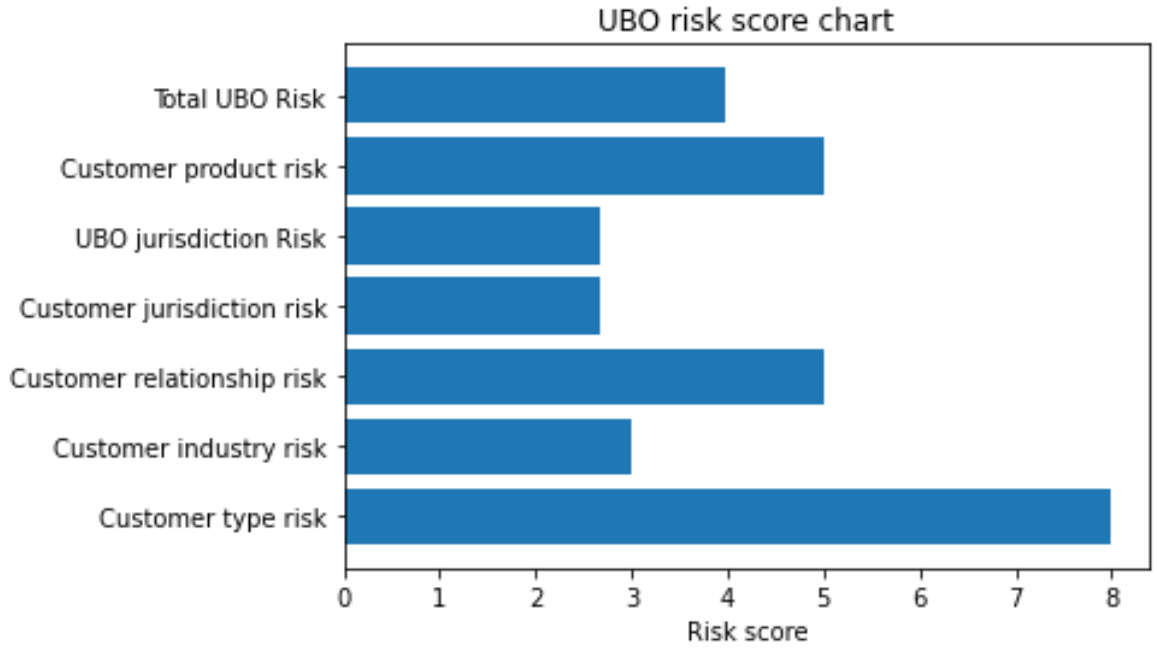

```
COMPANY AML TEST

Enter company name: LEIpapa OÜ
Enter company registration number: 16283000
COMPANY AML TEST LEIpapa OÜ 16283000
Company type risk
 1. Community interest company.
 2. Join-stock private company
 3. Listed company - EEA or equivalent
 4. Listed company - outside EEA or equivalent
 5. Partnership
 6. Private company limited by shares (Ltd.)
 7. Special purpose vehicle (SPV)
Enter company type: 6
Company type risk: 8
Choose company industry:
1. Advisory services
2. Aerospace
3. Agriculture
4. Arms
5. Automotive
6. Broadcasting
7. Chemical
8. Construction
9. Data exchange services
10. Defense
11. Education
12. Electronics
13. Energy
14. Entertainment
```

```
15. Escort services - dating
16. Financial services - crypto - not regulated
17. Financial services - crypto - regulated
18. Financial services - not regulated
19. Financial services - payment aggregators
20. Financial services - regulated
21. Fishing
22. Food
23. Gambling
24. Health care
25. Hospitality
26. Information
27. Insurance
28. Manufacturing
26. Marketing
27. Mass media
28. Mediation - car, water, air transport trade
29. Mining
30. News media
31. Petroleum
32. Pharmaceutical
33. Publishing
34. Pulp and paper
35. Real estate
36. Self Employed
37. Shipbuilding
38. Software
39. Steel
40. Telecommunications
41. Timber
42. Tobacco
43. Trade - electronics (export-import)
44. Trade - medicines
45. Trade - Precious metals
46. Trade - used cars, spare parts
47. Transportation and logistics
48. Travel agencies
49. Water
50. Wholesale
Enter company industry: 20
Industry risk: 3
Relationship risk
 1. New client, recent incorporated >1y, no previous bank account.
 2. New client, recent incorporated  1>3y, no previous bank account.
 3. New client, recent incorporated >1y, with previous bank account (TOP
50 EEA BANKS).
```

```
 4. New client, incorporated <3y, with previous bank account (NON TOP 50
EEA BANKS).
 5. New client, recent incorporated  1>3y, with previous bank account (TO
P 50 EEA BANKS).
 6. New client, incorporated <3y, with previous bank account (TOP 50 EEA
BANKS).
 7. Client 1-3 years
 8. Client 3+ years.
Enter customer relationship: 7
Relationship risk: 5
Enter company jurisdiction: ESTONIA
ESTONIA Country risk: 2.68
Enter company UBO country: ESTONIA
ESTONIA country risk: 2.68
Product type risk
 1. Fiat only.
 2. Fiat and Crypto exchange
 3. Fiat and Crypto transactions
 4. Crypto only
 5. Fiat and Crypto (Limited)

Enter product type: 1
Company product risk: 5
Total Company Risk: 3.972 low risk !!! NEED TO PERFORM EDD !!!
```



Source: LEIpapa OÜ