SUMMARY

Introduction to Risk Assessment

- The National Risk Assessment is an exercise to highlight the threats, vulnerabilities, and risks related to money laundering, terrorist financing, and proliferation financing as well as most common ways of laundering illicit proceeds or financing of terrorist acts in Estonia.

- This National Risk Assessment is Estonia's second risk assessment and covers the years 2017-2019. The National Risk Assessment is based on the World Bank's methodology, which was adjusted by PwC to fit the particularities of Estonia. 10 different working groups contributed to the National Risk Assessment with a total of 80 sectoral experts from the public as well as private sectors taking part in their work.

- In addition to document analysis and data collection, at the request of the Republic of Estonia Ministry of Finance, more than 6000 businesses, representatives of regulated professions, and non-profit associations completed a questionnaire concerning awareness of and experience with money laundering prevention, terrorist financing, and proliferation financing in the summer of 2020. The information obtained as a result of the exercise served as an important input for this National Risk Assessment.

- Cases related to money laundering that in the past took place foremost in the Estonian branch of the Danish banking group Danske but also in other banks have served as serious lessons to Estonia, bringing the money laundering prevention field under heightened governmental attention. These international cases demonstrated the strength of Estonian financial supervision – money laundering at Danske's Estonian branch was detected and stopped by the Republic of Estonia Financial Supervision Authority (Finantsinspektsioon). As a result of these cases that received a lot of public attention, supervision in Estonia's financial sector has become even more efficient in the last years, and the financing and capability of institutions involved in money laundering prevention has increased. Furthermore, the financial sector's knowledge of money laundering related risks has improved significantly in the past few years. Investments in solutions to detect money laundering and terrorist financing and in staff training have become more substantial, as have contributions to notifying the Financial Intelligence Unit.

- In a nutshell, the threats and vulnerabilities of the Estonian state as related to money laundering and terrorist financing are at an average level. On a five-point scale, Estonia's money laundering threat level is 2.40, while the nation's terrorist financing threat level is 2.09. Estonian state's money laundering vulnerability level is 2.73, while the terrorist financing vulnerability level is 2.67.

Money laundering risk

- There are domains in Estonia where money laundering and terrorist financing related risks are above average. The National Risk Assessment indicates that the greatest threats and vulnerabilities of money laundering and terrorist financing are related to businesses that operate in the field of virtual currencies as holders of an Estonian activity license. Until 2019, legislation that regulated the activities of businesses operating in the field of virtual currencies was overly lenient and this made it easier to obtain an activity license also for companies that had only minor connection to Estonia. Legislative amendments that took effect in 2020 have helped regulate this domain; however, the state needs to take quick additional steps to even better manage remarkable money laundering and terrorist financing risks related to the field.

- In the financial sector, the money laundering threat level is average. The greatest threats for the Estonian financial sector are related to moving funds through Estonian virtual currency service providers and via operations in countries other than Estonia by companies registered in Estonia by non-residents or e-residents. Further sources of threat include foreign trade related cash flows, services of company service providers, and tax evasion at both local and international level.

- During the National Risk Assessment, possible threats and vulnerabilities related to e-residents stood out in a number of fields. A significant amount of public and private services were available to potential e-residents also before launching of the programme, and e-residency ensures that the connection between a given operation and the person that performed it is identified with a significantly increased certainty. Consequently, e-residency as such will not, as compared to regular non-residents, bring along new risks. At the same time, e-residency potentially intensifies existing risks, making the conditions for the realisation of such risks more attainable if Estonia cannot sufficiently and operationally gather background information from the e-resident's country of origin or the country where their place of business is located. E-residency increases the country's vulnerability because it makes perpetration of violations of law simpler and cheaper.

- The Estonian state's vulnerability in relation to money laundering is slightly higher in the fields of real estate brokers, certain non-profit organizations, and company services providers. Vulnerability is reduced by increasing awareness so that obliged entities could recognise suspicious transactions and report them in a timely manner. There is also room for development in implementing confiscation measures, enhancing the work of supervisory authorities, and processing criminal offences connected to money laundering.

Terrorist financing risk

- The terrorist financing threat level in most fields in Estonia is low; the threat level is average in the financial sector and high in the domain of virtual currency. The country's vulnerability is above average in the non-profit sector among religious associations and charity organisations as well as in the financial technology sector among crowdfunding providers.

- The main difference between the nature of terrorist financing and money laundering is that while in the case of money laundering, a predicate offence must have been committed and assets must have been acquired by way of criminal activity, terrorist financing may take place involving assets of completely legitimate origin. An additional difference lies in proportions. In the case of money laundering, causing a serious outcome for the state presumes large monetary amounts and a wide scale while terrorist financing may be undertaken by smaller monetary amounts. By reference to the concept and nature of a terrorist offence, the assessment as pertaining to the dangerousness (to society) of a possible outcome of terrorist financing is always very high, even in cases where the relevant monetary amounts are small.

- As pertaining to the geographical threat of terrorist financing, it can be highlighted that the threat level is higher in the case of certain high-risk countries and conflict zones. Estonia considers associated high-risk countries to be nations with an Islamic regime or nations where fundamental Islam is widespread and in which are areas controlled by Islamic terrorist organisations and combative units.

Proliferation financing risk

- Proliferation financing risks are low in Estonia as a whole. Weapons of mass destruction and technologies and goods required for the weapons are not brought into Estonia and there have been no cases in Estonia where someone would have tried to use nuclear, biological, radioactive, or chemical material for an attack. In the past 15 years, no crimes related to proliferation of weapons of mass destruction or to proliferation financing have been detected. By virtue of valid EU and Estonian regulations and because Estonia is geographically located far from the transit routes of weapons of mass destruction, the probability of proliferation financing through Estonia is as a whole below average.

- Threats related to proliferation financing are above average in the field of virtual currencies. Virtual currency service providers are especially vulnerable due to the threat of violation of sanctions imposed on the Democratic People's Republic of Korea as it is known that during recent years the Democratic People's Republic of Korea has been using virtual currencies to earn illegal proceeds and circumvent the imposed sanctions.

Principal conclusions

- As one of the greatest weaknesses, the National Risk Assessment highlighted the fact that the Estonian state lacks sufficient capacity for strategic analysis in the field of money laundering and terrorist financing. Development of strategic analysis must be a state priority in the coming years.

- The lack of an administrative fine as a sanction continues to have a negative effect in Estonia on the efficiency of supervision of money laundering preventive measures. This does not enable to prescribe operatively proportional and effective sanctions in the case of an offence. Insufficient maximum fines also continue to be problematic as they are not in adherence to the European Union's directive on the prevention of money laundering.

- The quick resolution of extensive money laundering cases is hindered by the complexity and time-consuming nature of identifying predicate offences. Money laundering is by its nature exceedingly international and cooperation between investigative bodies and other countries to identify possible predicate offences, while oftentimes complex and time consuming as related to getting the required information, is of critical importance in identifying money laundering. National statistics, foremost criminal statistics, is often insufficient in this regard.

- In terms of different domains, the greatest risk lies with virtual currency service providers that hold an Estonian license, yet whose actual business operations have minimal connection to Estonia. The above are subject to high risk as pertaining to money laundering, terrorist financing, and proliferation financing. It is important, in cooperation with the private sector, to quickly reinforce the due diligence measures meant for virtual currency service providers so as to reduce the attractiveness of the virtual currency related environment for criminal abuse. The more stringent requirements for virtual currency providers that took effect in 2020 have not proven to be sufficient and the field remains insufficiently transparent.

- Implementing the relevant investments and IT solutions, virtual currency service providers are able to identify suspicious persons and transactions and report them to the relevant supervision. The required investments, competence, and motivation in the field as a whole are going up, but the level is uneven. It is important to increase the risk awareness of companies operating in the field as well as to achieve their greater contribution to the management of the relevant field-specific risks and to the development of appropriate regulations in order to ensure the legal functioning of the field.

- Exploitation of companies by criminal offenders is a continuing trend. Currently, there are no sufficient national control measures that would help prevent the creation of non-transparent chains of companies, concealment of the beneficial owner, and commission of violations of tax legislation. Obliged entities must therefore exercise due diligence and monitor the emergence of various indicators of abuse in order to mitigate the likelihood that risks associated with the exploitation of companies will materialise.

- Proposals for risk mitigation arising from identified national vulnerabilities – legislative amendments, preparation of guidelines, implementation of training, development activities, and allocation of resources. The proposals for action made on the basis of the National Risk Assessment will be consolidated in an action plan, the implementation of which will be supervised by the money laundering and terrorist financing prevention government committee.

Moving forward from the Risk Assessment

- During the implementation of the National Risk Assessment, it was revealed that the risk assessment based on the World Bank's methodology is in need of further methodological development in order to better meet the needs of the Estonian state next time.

- A quality leap is required in the extent of data collection, in the complex analysis of data in both strategic and tactical terms, and in the operativeness of the above. In terms of the relevant domains, the country's analytical capacity needs to be improved, among other things as pertaining to virtual currencies, real estate, business environment, and the non-profit sector but also in terms of the country's criminal statistics.

- Regarding the risk assessment process, its project-based nature needs to be reduced and the related processes need to be further integrated into the day-to-day organisational structures and operations of the fight against money laundering and terrorist financing.