



PREPARATION OF A RISK ASSESSMENT BY AN OBLIGED ENTITY

1 GENERAL INFORMATION ABOUT THE ASSESSMENT OF RISKS

With new legislation, *risk basis* has become a key element in the prevention of money laundering and terrorist financing.¹ Risk basis means that the parties subject to the reporting obligation identify, assess and understand the risks of money laundering and terrorist financing to which they are subjected in their own activities, and dimension their prevention measures required by the law according to such risks. The foundation for risk-based activities is a *risk assessment* made by the obliged entity concerning its own activity.

An obliged entity shall prepare a risk assessment to identify and assess the risks of money laundering and terrorist financing. The risk assessment shall be updated on a regular basis. The risk assessment and the changes made to it shall be supplied without undue delay to the competent supervisory authority or the bar association at their request.²

The party preparing a risk assessment must take into account the nature, size and scope of its own activities. Considering the factors mentioned above, the obliged entity must have sufficient operating principles, procedures and supervision to manage risks involving money laundering and terrorist financing.

The risk assessment helps the obliged entity plan for its operating principles, procedures and supervision such that they are in the right proportion to the risk in question. At the same time, the risk assessment also serves as a demonstration to the supervisory authority of the grounds on the basis of which the obliged entity has, in an individual case, decided on simplified or enhanced customer due diligence, for instance. The preparation of a risk assessment can be part of other risk management related to a customer relationship. Prevention of money laundering and terrorist financing can be regarded as a part of risk management, reliable administration and internal control of obliged entities.

These operating principles and procedures include, for example, practices related to risk management, customer due diligence and identification, reporting, storage of data, internal control and control of procedures, and review of employee activities. Obligated entities should ensure that their internal audit or other similar function tests such operating principles and procedures. Obligated entities should also make sure that they monitor and develop the operating principles, procedures and supervision referred to above.³

¹ The Act on Detecting and Preventing Money Laundering and Terrorist Financing (444/2017) entered into force on 3 July 2017, and it is based on Directive (EU) 2015/849 of the European Parliament and of the Council, issued on 20 May 2015, on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

² Money Laundering Act, Chapter 2, section 3(1)

³ Government proposal HE 228/2016, p.101

If the obliged entity is a legal person, the Board of Directors, general partner or another person in a similar position in senior management must approve the aforementioned operating principles, procedures and supervision, and monitor and develop measures related to them.

Supervisor-specific risk assessment

The Regional State Administrative Agency (RSAA) shall prepare an assessment of the risks of money laundering and terrorist financing among the obliged entities supervised by the agency. The assessment will be considered when planning the supervisory measures. In preparing the risk assessment, the RSAA shall have regard to:

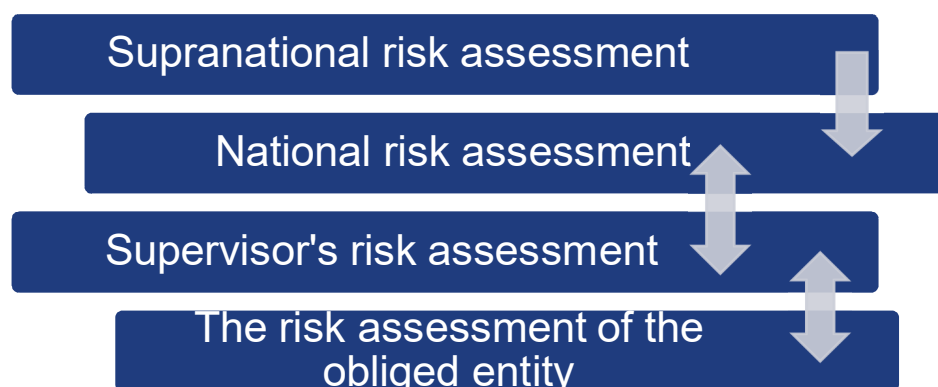
- 1) the European Union -wide assessment of the risks of money laundering and terrorist financing prepared by the Commission and the risks of money laundering and terrorist financing indicated in the assessment;
- 2) the national risk assessment and the national risks of money laundering and terrorist financing indicated in the assessment;
- 3) the risks of money laundering and terrorist financing concerning the sector supervised by the agency and relating to the obliged entities and to their customers, products and services.

The summary of the risk assessment shall be published for obliged entities to make use of it while preparing their own risk assessments. On the other hand, the information on sectoral risk factors specified in the risk assessments of obliged entities or discovered in the course of supervisory measures will be taken into account while preparing the RSAA's risk assessment.

National money laundering and terrorist financing risk assessment

The national risk assessment shall identify and assess the national risks of money laundering and terrorist financing. The assessment shall have regard to the European Union -wide assessment of the risks of money laundering and terrorist financing prepared by the European Commission (*Commission*). Among other things the purpose of the risk assessment is to provide the competent supervisory authorities, the bar association and obliged entities with information to support the preparation of their risk assessment.

The Ministry of the Interior shall publish a summary of the risk assessment. Before the summary is completed, the obliged entities may use the research on national risks published by the Police University College.



Upon preparing a risk assessment, the obliged entity should examine the following documents dealing with money laundering and terrorist financing:

- The EU's supranational risk assessment
- National risk assessment
- Summary of the risk assessment by the supervisory authority
- Annual report by the Financial Intelligence Unit

2 PREPARATION OF A RISK ASSESSMENT

1. **Identify threat factors and vulnerabilities for money laundering and terrorist financing related to your own business operations.**
2. **Plan and implement methods for preventing any threat factors and vulnerabilities detected.**
3. **Evaluate the remaining risk level, or *residual risk*.**
4. **Obtain the approval of the company's management for the risk assessment.**
5. **Make sure that the risk assessment is updated regularly and that the efficiency and timeliness of control methods with regard to the risks are assessed during such updates.**

2.1 Identification of threat factors and vulnerabilities

The first phase of the risk assessment is the identification of threat factors and vulnerabilities related to your own operation. You should start the process by listing the threat factors and vulnerabilities detected directly in your own operation or highlighted in the risk assessment by the supervisory authority or in the national risk assessment.

Threat factors

In identifying/evaluating threats of money laundering and terrorist financing, the obliged entity should take into consideration the risks of money laundering and terrorist financing related to their industry, products, services, technological advances as well as customers and their business operations.

Take the following factors into account, for instance:

- **Industry**
- **Customers**
- **Products and services**
- **Operating area (geographic)**
- **Business operations**
- **Distribution channels**
- **New technologies**

Vulnerabilities

Vulnerabilities are weaknesses occurring in the activities of a obliged entity that criminal operators can take advantage of an attempt to utilise for the purposes of money laundering or terrorist financing. Vulnerabilities can also be related to systems and operating models used by an obliged entity.

Take the following factors into account, for instance:

- **Resources**
- **Operating models/habits**
- **Systems**
- **Supervision**

2.2 Control methods

The second phase of the risk assessment involves charting the methods by which the party aims to control risks related to money laundering and terrorist financing or mitigate the effects of the realisation of such risks. Hence, the purpose of such control methods is to ensure that the risks detected are not realised, or that damage caused by the realisation of such risks can be minimised. These control methods can be related to, for instance, the systems and operating models used and related supervision.

When charting such control methods, attention should be paid to the following factors related to the processes, for example:

- **Customer identification and due diligence**
- **Storage of data (system support)**
- **Continuous monitoring**
- **Practices related to risk management**
- **Internal control**
- **Training of employees**

2.3 Residual risk

The outcome of the risk assessment by the obliged entity is called a “*residual risk*”. The residual risk is the risk of money laundering and terrorist financing that exists in spite of the control methods.

When assessing the residual risk, the obliged entity thus takes into consideration the threat factors and vulnerabilities identified and assesses the risk of being exploited for money laundering and terrorist financing, considering the risk management methods that the obliged entity has created in order to be protected against risks of money laundering and terrorist financing. The risk assessment should describe the chain of deduction from threat factors and vulnerabilities, through the control methods, to the residual risk.

The risk assessment should include a clear list of the conclusions, i.e., an assessment of the size of the residual risks, and the grounds for them.

2.4 Updates

The final phase of the risk assessment includes ensuring updates to the risk assessment and keeping the risk assessment up to date. The risk assessment shall be updated on a regular basis, for example annually and an entry shall be made about the update.

Changes can take place in threat factors and vulnerabilities when, for example, business operations are expanded to new geographical areas or to new areas of business. In the same context, the party should also evaluate the functioning and efficiency of the risk management methods with regard to the identified risks. The updating frequency can also be affected by, for instance, observations of new activity related to money laundering or terrorist financing, significant changes to the products or services provided by the obliged entity, or information on new risks related to money laundering or terrorist financing received from other sources.

Published: 14.11.2017

Updated: -