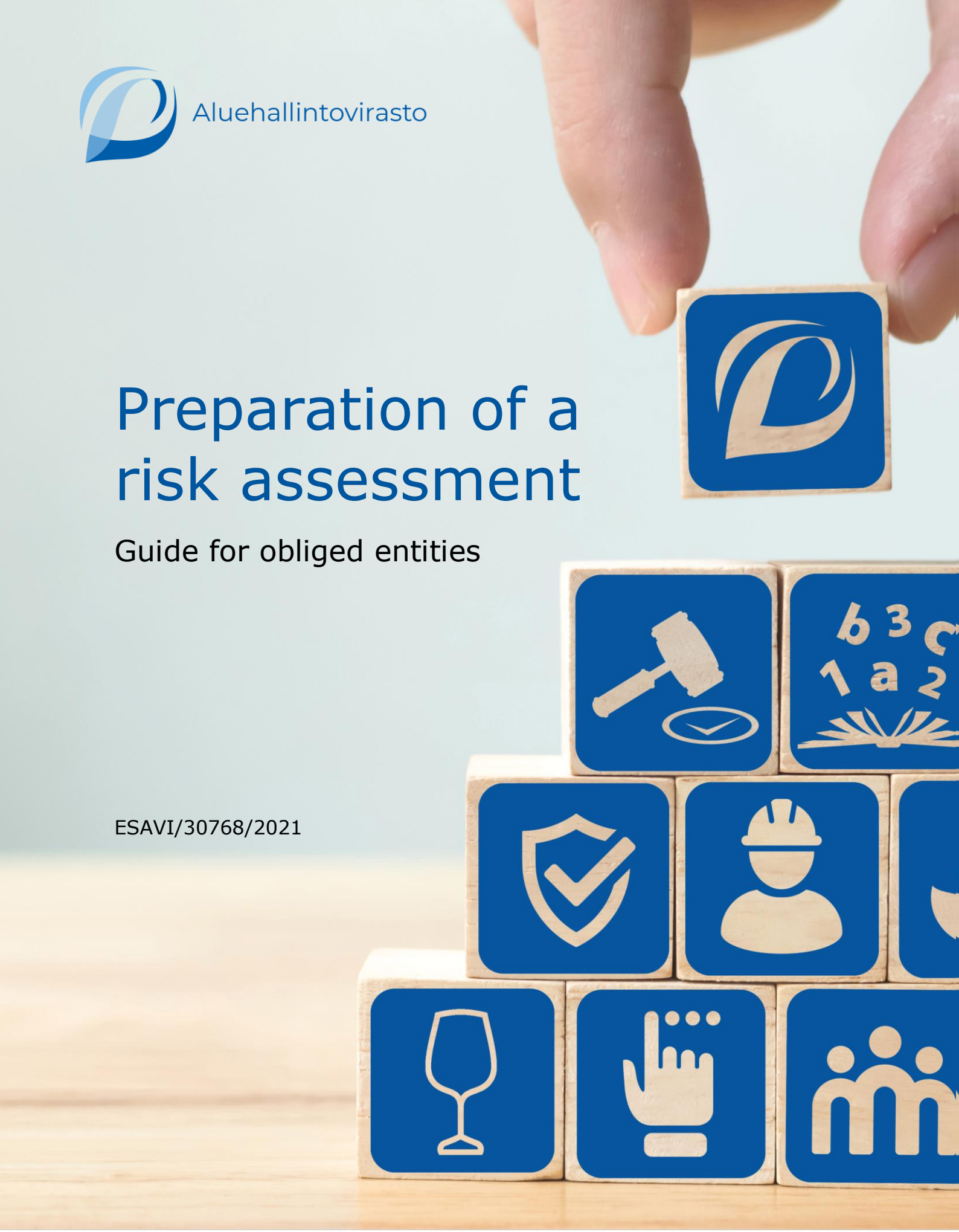
Aluehallintovirasto

Preparation of a risk assessment

Guide for obliged entities



ESAVI/30768/2021

Trade Enforcement

10/2021 Publications of the Regional State Administrative Agencies

Table of contents

1. Risk assessment – why?

1.1. What is a risk?

A **risk** is a possibility that a harmful or unwanted event occurs. It is a situation where it is possible, but not entirely certain, that a harmful event will happen with subsequent consequences. The risk of money laundering and terrorist financing refers to a combination of various threats, vulnerabilities and harmful consequences. Risks may be multinational, national or ones specific to an obliged entity, i.e. an actor with an obligation to report on issues covered by the Money Laundering Act.

Threats related to money laundering and terrorist financing include criminals, criminal groups, terrorist groups and persons involved in their operations (e.g. abettors) and objects. Threats may also include the typical practices of criminal actors in different types of offences (fraud, drug crime, financial crime, etc.). Criminal actors may seek to exploit vulnerabilities to succeed in money laundering or terrorist financing.

Vulnerabilities are weaknesses and shortcomings in e.g. the resources, operating methods, personnel competence, systems and internal supervision of a company that is an obliged entity. Vulnerabilities may also be associated with a company's products and services. These vulnerabilities can be exploited by criminal actors for money laundering or terrorist financing.

Money laundering refers to measures aimed at concealing or covering the origin of assets acquired through crime. Money laundering is preceded by a so-called predicate offence to acquire the assets that will be laundered. This means that in money laundering, suspicion is directed at the origin of the funds. Money laundering can be targeted at any criminal activity or outcome, such as money and assets acquired by criminal activity (e.g. funds acquired from drugs related crimes), the benefit generated by criminal activity (e.g. benefit obtained by tax offence) and the assets acquired in their place (e.g. property acquired by criminal funds).

Laundered property may be derived from any criminal activity. In Finland, money laundering is usually associated with fraud, theft, drug related crimes, crimes by debtors, tax offences and other financial offences. It is important to note that the amount of laundered assets may vary. Based on money laundering sentences issued in Finland, the value of laundered assets has varied from hundreds of euros to hundreds of thousands of euros. Money laundering can happen even if the assets concerned are not very large.

Once illegitimate assets have been successfully incorporated into the legitimate financial system and their criminal origin has been concealed or covered, the assets appear to be legitimately acquired. The crime of money laundering can also be committed by receiving, using, converting, transferring, conveying or possessing assets acquired through crime if the intent of the action is to gain a benefit to yourself or another party, to cover or conceal the criminal origins of assets or to aid the offender of a crime to avoid the legal consequences of an offence.

Terrorist financing refers to activities that provide or collect funds for a terrorist offence or for the financing of an individual terrorist or group of terrorists. In terrorist financing, the suspicion is focussed on the intended target of the funds, not the origin of the funds. Funds used for terrorist financing can also originate from legitimate sources. The funds may also consist of several small individual amounts. The crime of terrorist financing can be committed by someone who directly or indirectly gives or collects funds to finance terrorist acts or who knows that these funds will be used to commit terrorist offences, or to fund terrorist groups or terrorists as defined in legislation.

1.2. Why do risks need to be identified and assessed?

The purpose of a money laundering and terrorist financing risk assessment is that each actor within the scope of the Money Laundering Act, i.e. obliged entity, understands and assesses how their company's products and services could be used for money laundering or terrorist financing. The purpose is also to assess the ways in which an actor can reduce their risk of becoming an intermediary for money laundering or terrorist financing. These kinds of management measures may involve vulnerabilities and shortcomings whose impact must be assessed in relation to the identified risks. Obliged entities are key actors in combating money laundering and terrorist financing. By identifying and assessing risks to their activities, they will be able to establish procedures for detecting and preventing money laundering and terrorist financing.

Without a risk assessment, compliance with the obligations of the Money Laundering Act is not possible in practice. The Act requires that obliged entities conduct a risk-based customer relationship assessment and carry out risk-based customer due diligence throughout the customer relationship. Compliance with the risk-based measures is difficult if an obliged entity is not aware whether the risks of money laundering and terrorist financing are low, moderate, high or very high in the various aspects of the entity's business. Where the risk is highest, more effective measures and procedures are necessary to manage or reduce the risk. At the same time, the aim is to save low-risk operators from excessive bureaucracy.

A risk assessment does not mean the obliged entity demonstrating that it is not involved in money laundering or terrorist financing. The purpose of a risk assessment is also not to argue that risks are non-existent or that the activities carried out by the obliged entity are completely risk-free. A risk assessment is a toolset for the obliged entity to identify and assess the risks of money laundering and terrorist financing and to scale risk management measures accordingly. With a risk assessment, the obliged entity can also demonstrate to the Regional State Administrative Agency that the entity's procedures of customer due diligence and ongoing monitoring are appropriate to the risk level of money laundering and terrorist financing.

With the help of a risk assessment, the obliged entity can show the supervisory authority which criteria the entity has used in individual cases when deciding on matters such as a simplified or enhanced customer due diligence procedures. A

risk assessment and practical customer due diligence measures may not be contradictory; instead, the risk assessment must guide compliance with customer due diligence obligations.

1.3. What should a risk assessment include?

The Money Laundering Act does not stipulate any specific method or format for risk assessments. In order for the Regional State Administrative Agency to establish that a risk assessment in accordance with the Money Laundering Act has been carried out and that the obliged entity can demonstrate to the supervisory authority that the procedures of customer due diligence and ongoing monitoring are sufficient with regard to the risk of money laundering and terrorist financing, at least the following matters should be documented in the risk assessment.

A risk assessment must be drawn up **in writing**. Risk assessment templates are available, but a risk assessment must always be based on a careful assessment of the obliged entity's own operations. Pre-prepared, identical risk assessment templates created for large masses do not meet the requirements set for the risk assessment in the Money Laundering Act, but only serve as a template for the assessment of an obliged entity. For example, only filling in the company's name, sector and turnover in a risk assessment template is not enough.

When an obliged entity assesses the scope and extent of a risk assessment, they must take into account the **nature, size and extent of their activities**. The size and extent of activities refers to matters such as turnover and the number of employees and offices. The nature of activities includes what kind of business the company conducts and what types of products or services it offers to its customers. For example, an obliged entity with a high turnover and large number of employees must have a broader and more comprehensive risk assessment. On the other hand, small turnover alone does not necessarily mean that the risk assessment may be narrower, as factors related to the nature of the activities may require a broader risk assessment.

It is essential that a risk assessment covers the risks associated with a company's **products and services** as well as its **customers**. Risks associated with the products and services offered by a company can be assessed through related vulnerabilities and threats to determine the risk level typical of each product or service. When assessing the risks of money laundering and terrorist financing related to a customer relationship, relevant risks include ones related to new and existing customers, countries or geographical areas, ones related to new, developing and existing products, services and business transactions, as well as ones related to distribution channels and technologies.

A risk assessment should describe how it will impact compliance with the various obligations of the Money Laundering Act in practice. Based on the risk assessment, a company's customers can be classified with different risk categories, for example. An obliged entity can follow a simplified due diligence procedure if, based on a risk assessment, a customer relationship or an

individual business transaction involves a low risk of money laundering or terrorist financing. On the other hand, if a risk assessment indicates that a customer relationship or individual transaction involves an unusually high risk of money laundering or terrorist financing, the obliged entity has to apply the enhanced customer due diligence procedure. An integral part of a customer relationship risk assessment is setting up risk-based assessment procedures to establish the political exposure of a customer or a customer's beneficial owner. Risk-based procedures must also be established to identify and verify the beneficial owner.

In a risk assessment, an obliged entity must take into account the European Commission's list of high-risk countries for money laundering and terrorist financing and the lists of high-risk countries published by the Financial Action Task Force (FATF). FATF's black list of high-risk countries includes countries with serious strategic shortcomings in the fight against money laundering and terrorism. An enhanced procedure must be used with customers and transactions related to these countries and customer relationships, and transactions must be seriously considered. In turn, FATF's grey list includes countries that actively seek to remedy their strategic shortcomings in money laundering and terrorist financing prevention. A risk assessment must take into account possible links with countries on the grey list. Links to all abovementioned lists can be found in Chapter 3 of this guide.

Management measures and their assessment are an important part of risk assessment. Management measures refer to measures aimed at managing and reducing risks and preventing the exploitation of an obliged entity in money laundering or terrorist financing. In this respect, it is important to assess in particular what kind of vulnerabilities or shortcomings are associated with these management measures and how effective they are in reality. Management measures include various **internal operating principles, procedures and supervision**, and they must be sufficient in proportion to the nature, size and scope of an obliged entity's activities. Operating principles and procedures for example refer to practices related to risk management, customer due diligence, reporting, data storage, internal supervision, procedure supervision and reviewing employee activities. The functioning of an obliged entity's operating principles and procedures can be tested with internal audits or other similar means. Supervision does not have to categorically be realised as internal audits; instead, supervision can be carried out in a way that matches the nature, size and extent of an obliged entity's activities.

Internal operating principles, procedures and supervision must be monitored and developed. If an obliged entity is a legal person, the company's management must **approve the risk assessment** and the operating principles, procedures and supervision included in it.

A risk assessment provides information on any remaining risks that exist despite risk management measures. This kind of risk may also be referred to as **residual risk**. Residual risk can also be used to assess the overall risk level of money laundering and terrorist financing directed at the company and its business or professional activities.

A risk assessment must be **updated regularly**, for example when there are changes in the activities or customer base of an obliged entity. A risk assessment should include information on when it was updated and to what extent. When updating a risk assessment, it is also important to assess the effectiveness and timeliness of the risk management measures used by the company in relation to the identified risks. The need to update a risk assessment may also be impacted by factors such as the national risk assessment of money laundering and terrorist financing or a risk assessment conducted by a supervisory body.

A risk assessment can also include information on the person responsible for and the parties involved in preparing a risk assessment. The sources used in the preparation of a risk assessment should also be documented and, if necessary, accompanied by a description of how the different sources were utilised in the preparation of the risk assessment. An obliged entity must submit their risk assessment to the Regional State Administrative Agency on request without undue delay.

2. Preparing a risk assessment – how?

2.1. Risk assessment form

The format of risk assessments has not been specified. To assist in drawing up a risk assessment, an obliged entity may use the **risk assessment form** published by the Regional State Administrative Agency, or other similar documents. A risk assessment can also be prepared without using any risk assessment form, or a risk assessment form can be modified to match the company's operations. Various trade associations have drawn up risk assessment forms that are available for use.

When using different risk assessment forms, it is important to note that they only serve as a basis for an obliged entity's individual assessment. The purpose of the risk assessment form prepared by the Regional State Administrative Agency is for operators preparing risk assessments to identify and assess the risks related to money laundering and terrorist financing related to their own activities using the questions and instructions in the form. Pre-prepared, identical risk assessment templates created for large masses, where the obliged entity only fills in a few details like the company's name, sector and turnover, cannot be considered risk assessments compliant with the Money Laundering Act.

When preparing a risk assessment, a useful tool is the national risk assessment of money laundering and terrorist financing. It gives obliged entities information on the changing vulnerabilities, threats and risks of money laundering and terrorist financing. In addition, when preparing a risk assessment, it is important to look at documents such as the European Commission's Supranational Risk Assessment, the risk assessment summary by the Regional State Administrative Agency and other guidelines issued by the Regional State Administrative Agency. Looking into other external sources is also recommended. Chapter 3 of this guide lists information sources that are useful for preparing a risk assessment. The list is not exhaustive, so other sources can be used as well.

2.2. Risk identification and assessment

2.2.1. Products and services: vulnerabilities and threats

The first stages of preparing a risk assessment involve identifying risks related to a company's products and services. A good starting point is assessing the **vulnerabilities** related to products or services. Vulnerabilities refer to characteristics in products or services offered by a company that can make them vulnerable to money laundering or terrorist financing. The following factors can be assessed to identify vulnerabilities:

- availability of a product or service from the perspective of threats (criminal actors)
    - how easily or quickly a product or service is available to criminal actors
- the attractiveness of a product or service from the perspective of threats:

- anonymity for criminal actors
- mobility
- resale
- value retention

The degree of vulnerability can, for example, be assessed on a scale of 1 to 4, where 1 means that a product or service is not very vulnerable and 4 means that there are very significant vulnerabilities associated with a product or service. Justifying the assessment is important.

In addition to identifying and assessing vulnerabilities, it is also important to consider different **threats** and their significance. Threats can include criminals, criminal groups, terrorist groups and persons involved in their operations, as well as typical practices of criminal actors in different types of offences (fraud, drug crime, financial crime, etc.). The assessment of threats may include considering the possible ways and likelihood of criminal actors trying to use a company's products or services to conceal or cover the origin of funds acquired through crime. At the same time, it is also important to assess the possible ways and likelihood of criminal actors using a company's products or services to raise or send funds or other assets to finance terrorism.

When assessing the significance of threats, it is recommended to look at external sources, such as the national risk assessment for money laundering and terrorist financing, reports produced by police and intelligence authorities, and annual reports and other reports on various criminal phenomena and related threats.

The significance of threats can, for example, be assessed on a scale of 1 to 4, where 1 means that the threat level is low and 4 means that the threat is very significant. Justifying the assessment is important.

Comparing the levels of vulnerabilities and risks reveals the risk level associated with a product or service, or its **inherent risk**. For example, if a particular product or service is considered to be significantly (3) vulnerable and the significance of threats is low (1), the inherent risk level of the product or service is moderate (2). When assessing risk level, focusing on the vulnerabilities found in the products or services of a company is recommended. The vulnerabilities of a product or service can be assigned more weight in relation to their threats.

2.2.2. Products and services: risk factors

Preparing a risk assessment must involve assessing the different **risk factors** that affect the risks associated with a company's products and services. The number and quality of different risk factors affect the final risk level of the products and services offered by a company. Risk factors may indicate a low risk or a higher risk than usual, therefore affecting the inherent risk level of a product or service.

The impact of risk factors on the risk level of a product or service can for example be assessed as follows:

1. List the products and services offered by the company. Mark down their inherent risk level from 1 to 4, assigned at the beginning of the risk assessment process.

2. Assess the risk factors associated with each product or service as follows:

   - Customers
     - customer base of a product or service (e.g. private customers, small businesses, large enterprises, international companies, cash customers, others)
     - customers' lines of business
     - transaction types of customers buying a product or service (on-site transaction, non-face-to-face transactions, other)
     - connections of customers buying a product or service to different geographical areas and countries
     - nature of customer relationships of customers buying a product or service (e.g. permanent, one-off, other)

   - Business transactions
     - different payment methods for transactions (e.g. cash, credit transfers, debit cards, virtual currency, other payment methods)
     - location of business transactions (e.g. on-site, non-face-to-face, other)
     - identifying the purpose of business transactions and the origin of related funds (easy, reasonably easy, difficult, very difficult)
     - connections of business transactions to different geographical areas and countries
     - frequency and pace of transactions

   - Countries and geographical areas
     - High-risk states and regions listed by the European Commission and the FATF: ones whose actions to prevent money laundering and terrorist financing are not at a sufficient level
     - geographical area where a product or service is offered
     - location of the site where a product or service is offered

   - Distribution channels
     - different types and number of distribution channels
       direct sales to the end customer
       direct sales to retail
       sales through wholesalers
       sales through importers
       combination of several distribution channels

   - Technologies
     - product- or service-related payment and service methods and systems that utilise new technology
     - if the product or service itself is new technology

3. Assess the final risk level of the product or service on a scale of 1 to 4 once the impact of the risk factors has been taken into account.

It is also important to assess the impact of the sector-related risks associated with money laundering and terrorist financing on a company's operations. In this respect, it is advisable to look at materials such as the national assessment of the risk of money laundering and terrorist financing related to the company's sector and the justifications of this assessment and what impacts the risks in the sector have on the company's operations.

2.2.3. Customers

A risk assessment can also include an assessment of risk factors related to the different customer groups of a company. Risk factors refer to factors that may indicate a low risk or a higher risk than usual of money laundering or terrorist financing for each customer group. Identified risks will affect the customer due diligence procedures used by a company.

Different risk factors may be associated with different customer groups of an obliged entity. The customer base can be grouped in different ways, for example by dividing customers into private and corporate customers, and these groups can further be divided into various categories, such as small, medium and large corporate customers. Other grouping methods can also be used. Based on the risk factors assessed in the risk assessment, the risk levels of different customer groups may differ. One customer group may be low risk based on the associated risk factors, while another customer group may be high risk due to the identified risk factors and require an enhanced due diligence procedure.

Based on the risk assessment and identified risk factors, a risk profile or risk category can also be defined for individual customers and transactions. However, the risk assessment of individual customer relationships and transactions does not need to be included in a risk assessment; instead, it can be conducted in different ways, taking into account the size of the obliged entity's activities, for example by using information systems. When assessing the risks of money laundering and terrorist financing related to a customer relationship, relevant risks include ones related to new and existing customers, countries or geographical areas, ones related to new, developing and existing products, services and business transactions, as well as ones related to distribution channels and technologies.

Customer details that may indicate a low risk include:

- customer is a publicly traded company
- customer is a public entity or a public enterprise
- customer's place of residence or domicile is in a lower risk geographical area

On the other hand, a higher risk than usual may be associated with a customer:

- transaction is concluded in unusual conditions

- customer's place of residence or domicile is in a
    - country where, according to reliable sources, there is considerable bribery or other criminal activity
    - country with EU or United Nations sanctions, export or import prohibitions or similar measures
    - country that finances or supports terrorist activity or where known terrorist organisations operate
- personal funds are managed by a legal person or by legal arrangements
- company has a nominee shareholder or its shares are issued as bearer shares
- products and transactions may impede the identification of the customer or beneficial owner
- business operations involve a lot of cash payments
- company's ownership seems unusual or too complicated compared to the nature of the company's business operations

2.3. Risk reduction and management

An obliged entity must have adequate operating principles, procedures and supervision to reduce and effectively manage the risks of money laundering and terrorist financing. In a risk assessment, a company must examine the means at its disposal to manage and reduce the risks associated with money laundering and terrorist financing. Management measures can also be used to address the vulnerabilities related money laundering and terrorist financing identified by the company. Another important aspect of a risk assessment is to assess the extent to which management measures are not functional and effective enough to reduce and combat the risks of money laundering and terrorist financing, and to identify vulnerabilities and shortcomings in management measures.

When mapping management measures and related vulnerabilities, the following should be taken into account:

- Customer due diligence
    - company's internal processes and procedures for identifying and verifying customers and collecting due diligence data
    - documentation and retention of customer information
    - updating the customer due diligence data and ensuring that it is up to date
    - non-face-to-face identification policies

- Systems
    - money laundering and terrorist financing prevention systems are in place / are not in place
    - other systems are in place / are not in place
    - storing and documenting data in different systems
    - storing, backing up and restoring data in systems
    - usability and integrity of data stored in systems
    - organisation of document management and related responsibilities

- Continuous monitoring
  - manual or automatic (system-supported) continuous customer monitoring
  - monitoring permanent customer relationships
  - monitoring one-off customer relationships

- Practices related to risk management
  - regularly evaluating, revising and updating risk management practices and operating models
  - relationship between the risk management related to money laundering and terrorist financing and other types of risk management
  - documentation of risk management practices
  - available financial resources

- Internal control
  - efficiency and frequency of internal control
  - extending internal control to company's processes and practices for preventing money laundering and terrorist financing and to individual transactions
  - allocation of responsibilities for internal control

- Personnel training, competence and personnel resources
  - quality and quantity of training
  - responsibility for training
  - awareness of legislation and phenomena related to money laundering and terrorist financing
  - practical competence levels and ensuring competence
  - division of responsibilities in the prevention of money laundering and terrorist financing
  - personnel turnover, absences, new staff members

These example lists are not exhaustive, so new items can be added if necessary when preparing a risk assessment.

A risk assessment should also include a verbal assessment of the functioning and effectiveness of each management measure.

2.4. Assessment of residual risk

The final stages of a risk assessment involves assessing **residual risk**, i.e. the remaining risk level that exists in the company despite applied management measures.

The level of residual risk can be assessed as follows:

1. Assign risk levels.

2. Assess the impact of management measures on the risk level. Take into account any vulnerabilities and shortcomings identified in the management measures.
3. Assign numerical values to the level of residual risk (1 = low, 2 = moderate, 3 = high, 4 = very high) that remains despite the measures to mitigate risks.
4. Assess whether additional management measures are needed to further reduce the residual risk. If the residual risk is accepted without adding additional management measures, justify why the residual risk can be accepted without further measures.

In assessing residual risk, it is essential to clearly describe the chain of reasoning from identified risks to the risks remaining after management measures.

At the end of a risk assessment, the **overall risk level** of money laundering and terrorist financing on a company's business or professional activities can also be assessed based on the risks associated with the company's products, services and customer relationships. Justifying the assessment is recommended.

Figure 1. Risk assessment process

3. Additional information

European Commission's supranational risk assessment 2019

National risk assessment of money laundering and terrorist financing 2021

Summary of the risk assessment of money laundering and terrorist financing by the Regional State Administrative Agency

Instructions on reporting suspicious transactions – Regional State Administrative Agency guide for obliged entities

Prevention of money laundering and terrorist financing – Regional State Administrative Agency guide for obliged entities

High-risk third countries for money laundering and terrorist financing identified by the European Commission

FATF list of high-risk jurisdictions (black list)

FATF list of jurisdictions under increased monitoring (grey list)

Regional State Administrative Agency – Enforcement of the Anti-Money Laundering Act

Financial Intelligence Unit – Reviews and reports on combating money laundering and terrorist financing

Poliisi.fi – information on the most common crimes and criminal phenomena

Finnish Security and Intelligence Service Supo – Counterterrorism

Rahanpesu.fi – Prevent money laundering and terrorist financing

Regional State Administrative Agency for Southern Finland