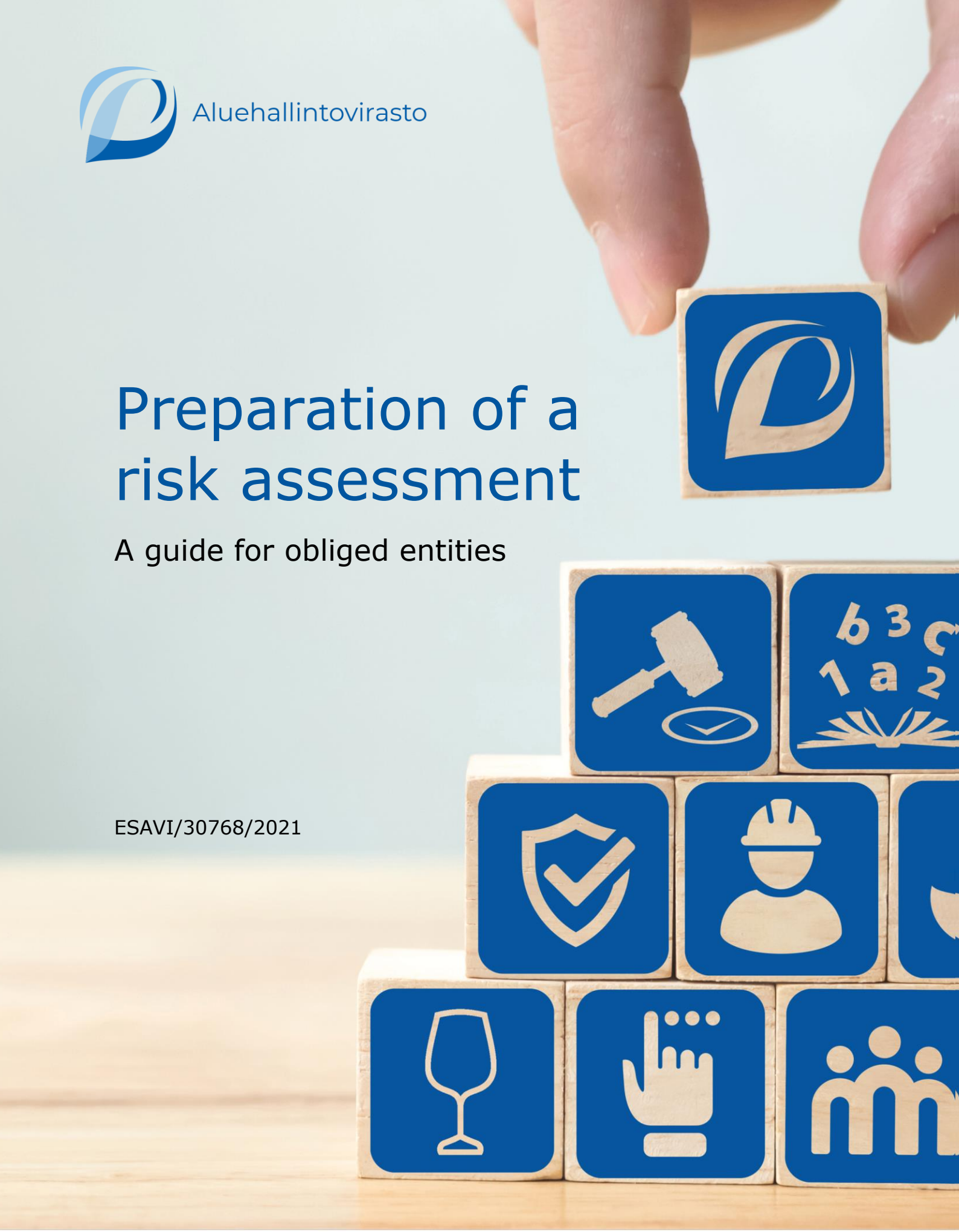
Aluehallintovirasto

Preparation of a risk assessment

A guide for obliged entities



ESAVI/30768/2021

Supervision of businesses

10/2021 Publications of the Regional State Administrative Agencies
Regionförvaltningsverkens publikationer

09/2024 Updated

Table of contents

1. Risk assessment – why? 1

1.1. What is a risk? 1

1.2. Why do risks need to be identified and assessed? 2

1.3. What should a risk assessment include? 3

2. Preparing a risk assessment – how? 6

2.1. Risk assessment form 6

2.2. Where to start? 7

2.3. Risk identification and assessment 9

2.3.1. Products and services: vulnerabilities, threats and other risk factors 9

2.3.2. Customers 14

2.4. Risk reduction and management 19

2.5. Assessment of residual risks 23

3. Additional information 26

1. Risk assessment – why?

1.1. What is a risk?

A **risk** is a possibility that a harmful or an unwanted event occurs. It is a situation where it is possible, but not entirely certain, that a harmful event will occur 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 supranational, national or ones specific to an obliged entity, i.e. an actor with an obligation to report on issues covered by the Anti-Money Laundering Act.

Threats related to money laundering and terrorist financing include criminals, criminal groups, terrorist groups and persons involved in their activities (such as 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 control 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 occur 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 offence 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 focused 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 Anti-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 methods 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 Anti-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 higher, 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 methods 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 continuous 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 procedure. 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 Anti-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 Anti-Money Laundering Act has been carried out and that the obliged entity can demonstrate to the supervisory authority that the customer due diligence measures and continuous 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.

The 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 activities**. Pre-prepared, identical risk assessment templates created for large masses do not meet the requirements set for the risk assessment in the Anti-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, business 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 a 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 the company can be assessed on the basis of the vulnerabilities and threats arising from them. When the risks of money laundering and terrorist financing related to a customer relationship are assessed, relevant risks also include the risks related to new and existing customers, countries or geographical areas, new, developing and existing products, services and business transactions as well as the risks related to distribution channels and technologies. An overall risk level can be determined for each product or service on the basis of threats, vulnerabilities and other risk factors.

A risk assessment should describe how it will impact compliance with the various obligations of the Anti-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 above-mentioned lists can be found in chapter 3 of this guide.

Management methods and their assessment are an important part of risk assessment. Management methods 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 methods and how effective they are in reality. Management methods 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 risk management practices, customer due diligence, reporting, data storage, internal control, 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 carried out 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 methods. This kind of risk may also be referred to as **residual risk**.

The 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 methods 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.

The risk assessment should also include the details of the person responsible for and the parties involved in preparing the 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 activities. 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 to ensure that the operators preparing risk assessments are able 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 Anti-Money Laundering Act. Particular attention should be paid to this because identical risk assessment models that the obliged entities have submitted as their own risk assessments account for a significant proportion of the risk assessments rejected by the Regional State Administrative Agency in its risk assessment supervision work each year.

There are many different ways to prepare a risk assessment and for this reason, in this chapter, the Regional State Administrative Agency provides obliged entities with general instructions on how to prepare a risk assessment. The chapter also contains instructions and illustrative examples for completing the risk assessment form provided by the Regional State Administrative Agency. Please note that the examples are completely fictitious and do not reflect the Regional State Administrative Agency's views on such matters as risks or risk levels in specific sectors.

In addition to the instructions issued by the Regional State Administrative Agency, obliged entities should also consult the national risk assessment of money laundering and terrorist financing when preparing a risk assessment. It contains information on the changing vulnerabilities, threats and risks of money laundering and terrorist financing. Obliged entities should also familiarise themselves with documents such as the European Commission's supranational risk assessment, and the risk assessment summary produced by the supervisory body of the Regional State Administrative Agency. Other external sources are also recommended. Chapter 3 of this guide lists information sources that are useful in preparing the risk assessment. The list is not exhaustive, which means that other sources can be used as well.

2.2. Where to start?

When preparing the risk assessment, first give the **basic details** of your company. Enter the name, business sector, turnover and the number of employees of your company as well as a description of the company, its activities, customer base and the geographical area where the company operates.

This basic information provides the basis for preparing the risk assessment because the activities carried out by the obliged entity, and their size and scope determine what should be included in the risk assessment. However, the basic details of the obliged entity are often missing, which means that the supervisory authority is unable assess the adequacy of the risk assessment on the basis of the risk assessment. For example, the risks facing the obliged entity and its obligations under the Anti-Money Laundering Act greatly depend on the number of persons employed by the obliged entity, which is why it must be stated in the risk assessment.

Figure 1. Example of how company details should be entered in the risk assessment form

Company details

Name of the company	Lakiasiaintoimisto Viljalti Oy Law Office
Business ID	1234567-8
Business sector(s)	Legal services
Turnover	EUR 4,600,000
Number of employees	21
Description of the company, its activities and customer base	Lakiasiaintoimisto Viljalti Oy Law Office was established in 2010. We have 18 lawyers and three other persons on our payroll. Our company has four shareholders, and we are specialised in a broad range of property and corporate law matters and labour law. The services that we offer are specified in the next chapter of the risk assessment. Most of our customers are Finnish companies or private individuals but about a quarter of our assignments have an international connection. Each year, we have about 400 customers of which 25% are continuous customers and 75% one-off customers. We do not manage criminal cases. About 65% of our assignments fall under the scope of the Anti-Money Laundering Act.
Operating area	We have offices in Turku and Vantaa. We manage assignments in Uusimaa and Southwest Finland and most of our customers are located in these two regions. However, our company has customers in all parts of Finland and we also have a small number of international customers in Germany and Sweden.

In addition to the basic details, the **details of the risk assessment** must also be given in the assessment. Enter the date on which the risk assessment was prepared and the details of the assessment updates. Also state if the risk

assessment has been examined but updates have not been considered necessary. The names of the person responsible for preparing the risk assessment and the parties that have taken part in the preparation of the assessment should also be given in the document. The date on which the management of the obliged entity has approved the risk assessment should also be entered in the document.

The obliged entity must have a clear internal process for preparing and updating the risk assessment. If you are preparing the risk assessment for the first time, also think how you should update the risk assessment in the future (for example, the frequency of the updates). Describe in the risk assessment the operating practices you have created to prepare the document.

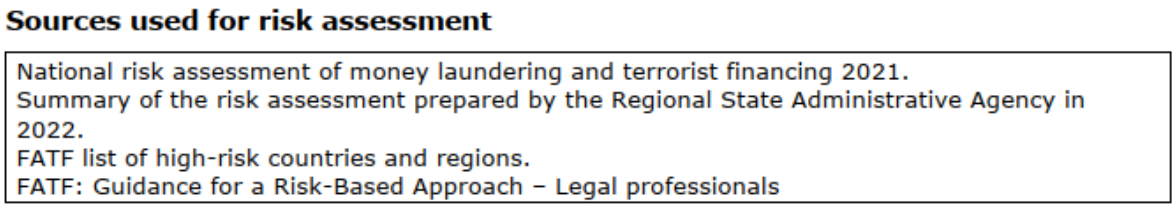
Figure 2. Example of how risk assessment information should be entered in the risk assessment form

Risk assessment details

Risk assessment prepared (date)	15 December 2021
Person responsible for preparing the risk assessment	Vilja Viekas, lawyer
Risk assessment was written by	Vilja Viekas, lawyer Tuomo Tunteva, KYC coordinator
Management approval	The risk assessment was approved by the Board of Directors at its meeting on 3 January 2022. The updates were approved on 5 April 2022 and 23 November 2023.
Preparation of the risk assessment	Vilja Viekas is responsible for preparing and updating the risk assessment. The KYC coordinator also participates in the preparation of the risk assessment. The need to update the risk assessment is assessed in November each year. If necessary, the risk assessment is also updated if, for example, there are changes in the company's activities or its operating environment. The updated risk assessment is presented and approved at the Board of Directors meeting following the updating.
Updates to the risk assessment	On 4 April 2022, risk factors associated with foreign customers and high-risk countries as well as risk management methods were updated. On 2 November 2022, the need to update the risk assessment was assessed, but no need for updates was identified after the additional update in April. On 3 November 2023, updates were made concerning the services offered by the company and sanctions.

The **sources** used in the preparation of the risk assessment should also be entered in the document. Updating the risk assessment is often easier if you have compiled a list of the sources. When updating the risk assessment, you should also take into account any updates made to the sources.

Figure 3. Example of entering sources on the risk assessment form



2.3. Risk identification and assessment

2.3.1. Products and services: vulnerabilities, threats and other risk factors

The first stages of preparing a risk assessment involve identifying risks related to a company's products and services.

The risks must be considered separately for each product or service falling under the scope of the Anti-Money Laundering Act. If you are using the risk assessment form provided by the Regional State Administrative Agency, you should add a sufficient number of tables on the form so that you can carry out the assessment. Also add an adequate number of rows for each product or service. Make sure that you are able to identify risks on a comprehensive basis and describe their relevance to your own activities. The risk assessment should not be a superficial document.

You can start the risk assessment by determining **vulnerabilities** associated with 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 the product or service is not very vulnerable, 2 means a moderate vulnerability, 3 means a significant vulnerability and 4 means that the product or service is associated with very significant vulnerabilities. Remember to give a verbal justification for the assessment, numerical assessment is not sufficient.

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 activities 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, you should also look at external sources, such as the national risk assessment of money laundering and terrorist financing, reports produced by the 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 is low, 2 means a moderate threat, 3 means a significant threat and 4 means a very significant threat. The assessment must also be justified verbally.

The Regional State Administrative Agency also specifically reminds parties to assess threats and vulnerabilities related to sanctions and the likelihood of their occurrence. With regard to sanctions, it is recommended that you describe and give reasons for the risks associated with the circumvention of sanctions can be linked to the company's operations or how the company's products and services can be used to circumvent sanctions.

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

The risk factors associated with each product or service can be assessed 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 (including the connection between the customer's transaction and the countries subject to sanctions)
  - 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 speed of transactions

– Countries and geographical areas
  - High-risk countries 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
  - sanctions risks

– 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

Also assess the level of the risk factor you have identified on a scale of 1 to 4, where 1 means that the risk factor is low, 2 means a moderate risk factor, 3 means a significant risk factor and 4 means that the product or service is associated with a very significant risk factor.

Even though vulnerabilities, threats and other risk factors are three different concepts, in the risk assessment form provided by the Regional State Administrative Agency, they are assessed in the same table one after the other. This is because in practice, treating them separately is often seen as difficult for such reasons as overlaps. As such, defining whether your company is affected by a vulnerability, a threat or other risk factors is irrelevant. The key issue is that you are able to identify the risk factors associated with your products and services, assess their relevance to your own activities and give sufficient justification for your assessment.

Figure 4. Example 1 of identifying and assessing risk factors associated with a product or a service in a risk assessment prepared by an obliged entity

1 Risk identification and assessment

1.1 Products and services: vulnerabilities, threats and other risk factors

Product or service: Pawnbroking

Risk factors associated with the product or service	Level
Our activities are associated with a significant vulnerability because the customer is often unable to present the original receipt of the pledge or any other reliable document about its origins. For example, we often receive old pieces of jewellery without original receipts in which case the possession of the items and the customer's description of their history are the only evidence of their ownership.	3
The services provided by pawnbrokers are seen as attractive by criminals because the items can be exchanged for money quickly and easily. This is also a major vulnerability of the services.	3
Even though we know many of our customers well, the risk is that parties that have committed different types of property offences use stolen or misappropriated items as pledges. Good customer knowledge reduces the risk, but if an ordinary item that fits the customer profile is offered as a pledge, and the description given by the customer is credible, illegally obtained items may not necessarily be identified.	3

Figure 5. Example 2 of identifying and assessing risk factors in a risk assessment prepared by an obliged entity

Customers making large cash payments are seen as a major risk factor. Typically, the largest cash payments are received from foreigners in whose countries cash payments are common or who find it difficult to make payments as credit transfers, for example. As a rule, foreign cash customers are associated with a higher risk because it is difficult to reliably trace the origin of the cash assets. The use of cash also involves a higher risk of circumvention of sanctions.	4
Distribution channels Most of the sales are made directly to customers. However, the resale of cars is relatively easy and quick, and they can be easily moved from one place to another. This makes the service and the product attractive to criminal actors.	3

It is also important to assess the impact of the risks associated with money laundering and terrorist financing on a company's activities. In this respect, it is advisable to look at documents 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 activities.

Figure 6. Example of considering the national risk assessment in the obliged entity's own risk assessment

National assessment of the risk of money laundering and terrorist financing in the company's sector and its potential impacts on your activities	Level
In the partial update of the national risk assessment of money laundering and terrorist financing (2023), the overall risk level for real estate agencies and housing rental agencies was estimated at 2 (moderately significant level). In the risk assessment prepared by the Regional State Administrative Agency, the risk level of real estate agencies is estimated at 3. The threats, vulnerabilities and other risk factors identified in the national risk assessment have been taken into account in our activities, and they are combated with adequate risk management methods (such as customer due diligence measures, personnel training and internal control). We have also introduced additional guidelines and risk management methods to ensure compliance with sanctions.	2–3

Now that you have comprehensively identified and assessed risk factors associated with a product or a service, you should next turn your attention to the **overall risk** arising from the product or the service. The overall risk can be determined by making comparisons between the levels of vulnerabilities, threats and other risk factors associated with a product or a service and the justification for them. When assessing risk levels, you should pay particular attention to the vulnerabilities found in the products or services of your company. The vulnerabilities of a product or service can be assigned more weight in relation to threats associated with them. Other identified risk factors must also be taken into account in the overall risk level assessment.

Figure 7. Example of the assessment of the overall risk associated with a product or a service

Assessment of the overall risk associated with the product or the service	Risk level
Real estate agency Kukkanen Oy has identified several vulnerabilities above and, as a rule, they are all considered as lowly or moderately significant. Only one vulnerability is considered significant (3). In our activities, we also face some of the threats assessed above and considering their likelihood, they are deemed as moderately significant (2). We have also comprehensively assessed other risk factors that may relate to our transactions (2), our customers (1–3) and geographic areas (1). Even though as a rule, risk factors are at level 1–2, we have occasionally dealt with concrete risks in our operations and submitted reports on suspicious transactions. We have also taken into account such factors as the national risk assessment, and we believe that our risk management methods provide an adequate response to the risks described in it. Based on the identified vulnerabilities, threats and other risk factors, we estimate that the level of risk associated with our brokerage business is moderately significant (2).	2

2.3.2. Customers

The risk assessment should be an assessment of the risk factors associated with the different customer groups of the company because, ultimately, the risk of money laundering or terrorist financing arises from the activities of the obliged entity's customers. Risk factors refer to factors that may indicate a low or higher -than-usual risk of money laundering or terrorist financing for each customer group. Identified risks will affect the customer due diligence procedure used by a company.

Different customer groups of an obliged entity may be associated with different risk factors. 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 should also be used because otherwise, the risk assessment may remain too general. For example, accounting firms should group and assess risks associated with their customers on the basis of the sectors in which they operate. For example, in some areas, the customer's operating environment may be highly significant and thus also excellently suited for grouping.

Figure 8. Example of identifying and assessing risk factors associated with customers in a risk assessment prepared by an obliged entity

1.2 Customers

Customer group	Assessment of risk factors	Risk level
Customers seeking damages (20% of our customers)	As a rule, cases involving disputes and damages are not particularly risky but they may involve a clear risk of abuse. Particularly high-risk assignments include those in which the lawyer suspects a fictitious dispute or grounds for damages and in which the dispute is resolved relatively quickly and/or the compensation to the other party is paid through a trust account. At annual level, about one fifth of our assignments involve customers seeking damages. Last year, a total of 83 customers were provided with services related to damages. About 35% of these customers were long-term clients and we estimate that in their case, the risk of abuse is lower. A total of 65% of the customers seeking damages were one-off clients and they are generally associated with a higher money laundering risk. Two categories of one-off assignments were identified as particularly risky: cases in which the damages were paid to our trust account (8 cases) and the cases in which the reason for the damages or for using our services remained unclear (2 cases).	2
Housing companies (about 5% of our customers)	The revenue of housing companies consists of charges for expenses and their activities are not seen as a particularly effective way of money laundering. We rated the risk associated with housing companies as lowly significant. In most cases, housing companies are also long-term customers, which makes it easy to monitor their activities. At the moment, we have 15 long-term housing company customers. During the past year, we have had five housing companies as one-off customers.	1
Private traders	The risk level of private traders is associated with factors	2

Based on the risk factors assessed in the risk assessment, the risk levels of customer groups may differ. One customer group may constitute a minor risk based on the associated risk factors while another customer group may constitute a high risk due to the identified risks 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 the 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-than-usual risk may be associated with a customer if

- the 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 subject to 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 operation involve a lot of cash payments
- company's ownership seems unusual or too complicated compared to the nature of the company's business operations

After you have identified and assessed risk factors associated with your customers you should determine their impact on complying with customer due diligence obligations.

Figure 9. Example of complying with simplified and enhanced due diligence procedure on the basis of a risk assessment prepared by an obliged entity

How does the risk assessment affect compliance with customer due diligence obligations?

Simplified due diligence procedure	For practical reasons, our company does not have any simplified due diligence procedure.
Enhanced due diligence procedure	The enhanced due diligence procedure is applied to politically exposed customers and customers that have a connection with a high-risk country. The enhanced due diligence procedure is also applied to accounting firm customers whose risk level is estimated at 3 or 4 (high-risk customers) in the above assessment. Records are kept of the customers falling under the scope of the enhanced due diligence procedure. There are currently 38 customers falling under the scope of the enhanced due diligence procedure and thus also under the scope of enhanced continuous monitoring. The accuracy of the due diligence data on the customers falling under the scope of the enhanced due diligence procedure is reviewed every 6 months. Specific transactions are also subject to particularly extensive and thorough monitoring. For example, the background and basis of each transaction that has a connection to a high-risk country is examined with particular care. The same applies to transactions considered as particularly risky on other grounds. In addition to the transaction receipt, we always request the customer to give us access to the agreements on which the transaction is based. If necessary, we report suspicious transactions with a low threshold. The enhanced due diligence procedure is discussed in more detail in our

Note that the obliged entity must have the appropriate risk-based procedures in place to determine whether a customer or their beneficial owner is or has been a politically exposed person, a family member of a politically exposed person, or an associate of a politically exposed person. This means that in its risk assessment, the obliged entity must assess the need to investigate the political exposure of the customer, methods of investigating the matter and the risk management methods used in connection with politically exposed customers. Unfortunately, customers' political exposure and the associated measures are only rarely discussed in the risk assessments submitted by the obliged entities supervised by the Regional State Administrative Agency.

Figure 10. Example of risk-based assessment of PEP procedures in a risk assessment prepared by an obliged entity

Politically exposed persons	According to our assessment, politically exposed persons may be associated with a higher risk of money laundering due to possible corruption. Even though there are probably no corrupt PEPs among our customers, the risk cannot be completely ruled out. For this reason, our company uses risk-based procedures to determine a person's PEP status. We check the PEP status of our pawnbroking customers when the total value of the pledges made on one occasion or in several instalments is at least EUR 500. Our estimate is that the risk of corruption among our customers is fairly low because a large proportion of the pledges are ordinary pieces of jewellery and household articles of low value brought to us in small numbers. We estimate that the risk of corruption is mainly associated with transactions of higher value and for this reason, it is not necessary to check the customers' PEP status in connection with the lowest-value transactions. We estimate that buying pawned items at an auction involves a lower risk of corruption than using items as pledges. Therefore, we only check the PEP status of the persons buying pawned items when the cash payment exceeds EUR 500. When the item is paid with a card or as a credit transfer, the customer's PEP status is checked if the amount of the payment exceeds EUR 3,000. The customer's PEP status is checked by asking the customer about the matter, and if necessary, the information can also be obtained from other sources. The PEP status is entered in the customer details. Politically exposed persons fall under the scope of the enhanced due diligence procedure. We always ask customers falling under the scope of

A number of other customer due diligence measures are also based on risk-based assessment. For example, the identity of the customer's beneficial owners must be checked *if necessary*. Typically, at least high-risk customers meet the requirement for necessity. The verification of the identity of the beneficial owners should be addressed in the risk assessment.

Figure 11. Example of the addressing of the verification of beneficial owners' identity in the risk assessment

Verifying the identity of beneficial owners	As a rule, the identity of the beneficial owners is not verified unless the beneficial owner is also the customer's representative. The identity of all high-risk customers and their beneficiaries is always verified when an agreement is concluded and when changes are made to the details of the company's responsible persons during the customer relationship. The identity of the customer's beneficial owners is also verified if there are unclarities concerning the matter or if the verification is justified for other reasons.

The effectiveness and adequacy of the sanctions procedures of the party subject to the reporting obligation must be assessed in the risk assessment. Taking sanctions and frozen funds lists into account is an absolute part of customer due diligence and cannot be bypassed on the basis of a risk assessment However, a risk-based approach can be used to direct and plan resources, which allow for compliance with sanctions regulation and national freezing orders. However, risk-based consideration cannot be used to determine whether or not the company complies with sanctions regulation and national freezing orders- All parties subject to the reporting obligation must have procedures in place to ensure that they do not violate sanctions or freezing orders in any situation.

Figure 12. Example of the addressing of sanctions and freezing orders in the risk assessment

Sanctions and freezing orders	We comply with sanctions regulation and national freezing orders in full. We do not provide accounting services to entities established in Russia or to Finnish companies whose beneficial owners are on the sanctions list. We also do not serve customers who are themselves or whose beneficial owners are on the sanctions list or frozen funds list. Procedures for ensuring compliance with sanctions and freezing orders are discussed in separate written guidelines and in this risk assessment's section on risk management methods. Based on the risks identified in the previous section, we have allocated more resources to monitoring those customers that we believe are at increased risk of circumventing sanctions. Enhanced due diligence and, in particular, enhanced continuous monitoring cover all customers who have engaged in Russian trade or other transactions with sanctioned entities over the past ten years. In order to detect the circumvention of sanctions, we pay particular attention to transactions that are similar to those that our customers have previously carried out with entities established in Russia, even if the transaction were to now take place with another company or state. We will make all transactions with a connection to a

2.4. 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 methods can also be used to address the vulnerabilities related to money laundering and terrorist financing identified by the company. Another important aspect of a risk assessment is to assess the extent to which the management methods are not adequately functional or effective to reduce and combat the risks of money laundering and terrorist financing, and to identify vulnerabilities and shortcomings in the management methods.

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

- Customer due diligence

  - company’s internal processes and guidelines 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

- Procedures for complying with sanctions regulation and freezing orders
  - operating principles, practices and internal controls for complying with sanctions regulation and freezing orders;
  - sanctions monitoring
  - the effectiveness, adequacy and temporal dimension of sanctions procedures
  - sufficient resources

- 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 and obligation to obtain information
  - manual or automatic (system-supported) continuous customer monitoring
  - monitoring permanent customer relationships
  - monitoring one-off customer relationships
  - obligation to obtain information on specific transactions

- Risk management practices
  - 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

- High-risk customers
  - procedures to reduce risks arising from high-risk customers

- 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.

A risk assessment should also include a verbal assessment of the functioning and effectiveness of each management method. In the verbal assessment, risk management methods could be characterised as "functional", "moderately functional", "inadequate" or "very inadequate".

Figure 13. Example of the addressing of risk management methods in a risk assessment

2 Money laundering and terrorist financing risk management methods

Risk management methods		Functionality of the management method
Customer due diligence	We perform all due diligence measures required under the Anti-Money Laundering Act. The due diligence measures are described in a separate process diagram and in our internal guidelines. All customers fall under the scope of normal or enhanced due diligence procedure. Customers falling under the scope of the enhanced due diligence procedure and the methods applied to them are assessed in chapter 1 of the risk assessment.	**functional**
Compliance with sanctions regulation and decisions on the freezing of funds	As part of the customer due diligence process, we ensure that the customer, their business or other business-related parties are not on the sanctions or frozen funds lists. We conduct a sanction list check of all contractors or their beneficial owners whenever a customer relationship is established. In addition, a sanctions list check is carried out on all parties involved in the transaction (clients and their counterparties) whenever a real estate agent receives or forwards a new purchase offer. A final check of sanctions lists is carried out when the seller and buyer have agreed on finalising a transaction and the transaction is carried out. The checks are carried out manually by comparing the names of the customer and their beneficial owners with the lists. We record the time and result of the sanction list monitoring in the customer data. We are introducing a system that searches these lists automatically and regularly. Although we have	**functional**

Figure 14. Example of the addressing of risk management methods in a risk assessment

Internal control	Internal control of compliance with the obligations laid down in the Anti-Money Laundering Act is the responsibility of Tarmo Tarkastaja, head of the KYC team and a shareholder of our company. His tasks include ensuring that all customer due diligence data required by law and described in this risk assessment and our internal guidelines has been appropriately obtained on each customer and that the necessary KYC information has been obtained before the transaction is carried out. The supervisor is responsible for ensuring that the company follows uniform operating practices, for example in situations where suspicious transactions are identified. Internal control is carried out by means of monthly system runs and manual spot checks. A report on the checks performed and the quality deviations identified in them is prepared and the document is discussed at the Board of Directors meeting and the personnel meeting.	**functional**
Continuous monitoring and obligation to obtain	As a rule, our customers perform one-off assignments or transactions where	**moderately functional**

The lists of examples described above are not exhaustive and thus when a risk assessment is prepared, information can be added to them or other changes can be made to them. For example, you can consider how risk management methods can be used to accurately respond to a significant risk that you have identified.

Figure 15. Example of how risk management methods addressing a specific risk can be described in a risk assessment

Risk management methods		Functionality of the management method
The customer uses cash of illegal origin to buy valuable jewellery	When the cash payment exceeds EUR 1,500, we always ask the customer to provide an oral account of the origin of the money. The oral account is entered in the customer due diligence form. The employee must pay attention to the credibility of the account given by the customer. If the account is credible, the transaction can take place. To support the account provided by the customer, we obtain documents to verify the accuracy of the account. For example, if the customer claims that the money is earned income withdrawn from an account, the employee must ask the customer to provide an account statement showing the earned income and the cash withdrawal. In that case, the account statement is added to the customer details. If no reliable information can be obtained but the account provided by the customer is credible, we will carry out the transaction and will immediately report it as a suspicious transaction to the Financial Intelligence Unit. If the account given by the customer is not credible or the transaction is inconsistent with the customer profile and no reliable information is available to support the customer, we refuse to carry out the transaction. In that case, too, we will report the matter to the authorities if the customer's name is known.	**Moderately functional**

2.5. Assessment of residual risks

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 methods.

You should start the examination of the residual risk by assessing the impact of available risk management methods on the product or service and the risk level of its customers. Take into account any vulnerabilities and shortcomings identified in the management methods.

You can, for example, assess the residual risk level on a numerical basis on a scale of 1 to 4. However, you should pay particular attention to the verbal assessment of the residual risk.

Once you have completed the assessment of the residual risk, assess whether additional risk management methods are needed to address the remaining risk so that the risk can be further reduced. If the residual risk is accepted without any additional management methods, explain in writing why the residual risk can be accepted without additional measures.

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

Figure 16. Example of assessing residual risks in a risk assessment

3 Assessment of residual risk

Product or service: Pawnbroking

Assessment of residual risk	**Acceptability of residual risk**
The risk management methods applied by our company (such as customer due diligence, checking the origin of funds and our own professional skills) significantly reduce the risks and the likelihood that they are materialised in our operations. Despite effective risk management methods, there is always a moderate residual risk that we accept illegally acquired property if in terms of its amount or quality, the pledge, such as a piece of gold jewellery, is unexceptional and fits the customer profile.	The residual risk must be accepted as it cannot be completely eliminated with additional risk management methods. We consider it likely that the residual risk may materialise at some point. For example, requiring the original purchase receipt for each individual item would be an exaggeration as it would prevent the conduct of business almost entirely. Introducing more comprehensive risk management methods would be impracticable and the existing residual risk must be accepted.

Figure 17. Process of preparing a risk assessment

3. Additional information

European Commission’s supranational risk assessment 2022

National risk assessment of money laundering and terrorist financing 2021

National risk assessment of money laundering and terrorist financing 2023 – partial update

Supervisor-specific risk assessment prepared by the Regional State Administrative Agency for Southern Finland under the Anti-Money Laundering Act 2023 – public summary (in Finnish)

Guidelines 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

European Commission’s list of high-risk countries outside the European Economic Area

Black and grey lists of FATF

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

Training videos of the Regional State Administrative Agency, YouTube channel containing information on enforcing the Anti-Money Laundering Act (in Finnish)

Financial Intelligence Unit – Reviews and reports on combating money laundering and terrorist financing (in Finnish)

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