Federal Ministry
Republic of Austria
Finance

National risk assessment 2025



Imprint

Media owner, publisher and editor:
Federal Ministry of Finance, Johannesgasse 5, 1010 Vienna
Vienna, 2025. Status: 2. Juni 2025

Copyright and liability:
Excerpts may only be reprinted if the source is acknowledged; all other rights are prohibited without the written consent of the media owner
It should be noted that, despite careful editing, all information in this publication is provided without guarantee and the Federal Chancellery and the author accept no liability. Legal statements represent the non-binding opinion of the author and can in no way prejudge the jurisdiction of independent courts.

Foreword


Harald Waiglein, Msc.

Ladies and Gentlemen,

Money laundering, terrorism financing and proliferation financing have remained extremely present challenges in recent years. Prevention systems against money laundering make it more difficult for criminals to profit from their activities. Measures against terrorism financing make it possible to disrupt financial flows for terrorist attacks and to identify terrorist groups. Combating proliferation financing prevents dangerous states from developing nuclear weapons. Effective control systems also strengthen the reputation of companies and thus contribute to Austria's competitiveness as a business location.

This National Risk Assessment is an important basis for measures to prevent money laundering and terrorism financing. It is intended to enable authorities and obliged entities to deploy their resources in a targeted manner and take effective preventive measures. The National Risk Assessment is the joint results document of all authorities involved in preventing and combating money laundering and terrorism financing in Austria.

We were able to update and expand the National Risk Assessment 2021. In addition to a horizontal overview of national risks, we are adding two cross-sector analyses, a horizontal anchoring of proliferation financing risks and a chapter on protecting the NPO sector from misuse for terrorism financing.

The National Risk Assessment is intended to contribute to a better understanding of risk by all the authorities concerned and the private sector and thus lead to a more effective fight against money laundering and terrorism financing in Austria. The Federal Ministry of Finance is committed to the implementation of international and European standards to combat money laundering and their continuous further development with its European and international partners.

Harald Waiglein, Msc.
Head of Section III - Economic Policy and Financial Markets

Contents

Foreword 3

1 Executive Summary 6

1.1 Money laundering 6

1.2 Terrorism financing 7

1.3 Proliferation financing 9

2 Introduction 11

2.1 Objectives of the National Risk Assessment 11

2.2 Preparation of the National Risk Assessment 12

2.3 Methodology 13

3 Money laundering threat scenarios 14

General description and database 14

3.1 The concept of "predicate offence" 14

3.2 Data basis for the risk assessment 15

4 Threat scenarios for terrorism financing 31

5 Threat scenarios for proliferation financing 37

6 Cross-sector risks in the property sector 46

7 Cross-sector risks of means of payment and payment and financial transfer systems 55

8 Sectoral risk assessment of legal entities and trusts 63

8.1 Domestic legal entities 63

8.2 Foreign legal entities 109

9 Financial sector 129

10 Sectoral risk assessment of the legal profession 163

11 Sectoral risk assessment notaries 171

12 Sectoral risk assessment of tax consultants and auditors 180

13 Sectoral risk assessment of accounting professions 195

14 Sectoral risk assessment gambling 204

15 Sectoral risk assessment for tradespersons 222

15.1 Insurance intermediaries 222

15.2 Office services; Management consultants 227

15.3 Trade incl. auctioneers 231
a) Antiques and works of art 231
b) Precious metals and precious stones 236
c) High-priced goods - other than precious metals and precious stones 240
15.4 Real estate agents 244
16 Sectoral risk assessment of non-profit organisations 252

1 Executive Summary

The basis of all **measures** to prevent money laundering and terrorism financing taken by the authorities and obliged entities in the private sector is the **risk-based approach**. This requires a **comprehensive understanding** of the **national risk landscape**. The aim of the National Risk Assessment is to create such a basis.

1.1 Money laundering

Money laundering methods are diverse and numerous. The methods highlighted here have emerged in particular from analyses and proceedings conducted by the A-FIU and the Federal Ministry of Finance. Incriminated funds must always be laundered, regardless of the predicate offence. The further development of technical possibilities also opens up new opportunities in the world of money laundering. For example, forms have emerged in the area of virtual currencies or cryptoassets that enable greater concealment of identities or minimise market value risks.

Other possibilities include infiltration into companies and the use of offshore constructs in the background. In the construction industry in particular, there have been perceptions for several years that company constructs are being used to pass on money by means of kickback payments and fictitious invoices, which are ultimately used to pay illegal wages in cash.

However, it should also be emphasised that there are other methods of money laundering that have received less attention to date. One of these is the practice of investing incriminated funds in life insurance policies for the purposes of money laundering. This method is of particular interest as it allows large sums to be invested without being entered in a register accessible to the authorities. Meanwhile, other familiar forms such as hawala or property have also come to stay.

Frequency of the predicate offence:

very common	frequently	regularly	rare
fraudulent offences	Offences related to documents	tax related predicate offences	organised crime
		smuggling	human trafficking/smuggling
		social benefit fraud	sanction violations
		drug-related crime	corruption

Money laundering methods:

very high	high	medium	low
bogus companies	offshore	life insurance	
Fraudulent offences	virtual currencies and cryptoassets	online accounts	
	luxury goods		
	real estate		
	prepaid cards		
	hawala		

Sectoral risks of money laundering:



Austria's geographical proximity, particularly to the countries of the Western Balkans, and existing family ties can facilitate the transfer of assets of criminal origin to these countries.

1.2 Terrorism financing

The financing of terrorism is currently limited primarily to maintaining the organisation of terrorist groups. The leadership of such a group, even if it is not located in a crisis area, requires financial resources for strategic tasks such as propaganda, recruitment of new members and to cover the

organisational costs and living expenses of the cadres. After Austria was the target of terrorist attacks in the 1970s and 1980s, it then developed into a transit and retreat country where financing, recruitment and propaganda were carried out. The terrorist attack on 2 November 2020, but also foiled attack plans such as on the Rainbow Parade 2023, New Year's Eve 2023 and the Taylor Swift concert in 2024, show that Austria is once again a target country for terrorism.

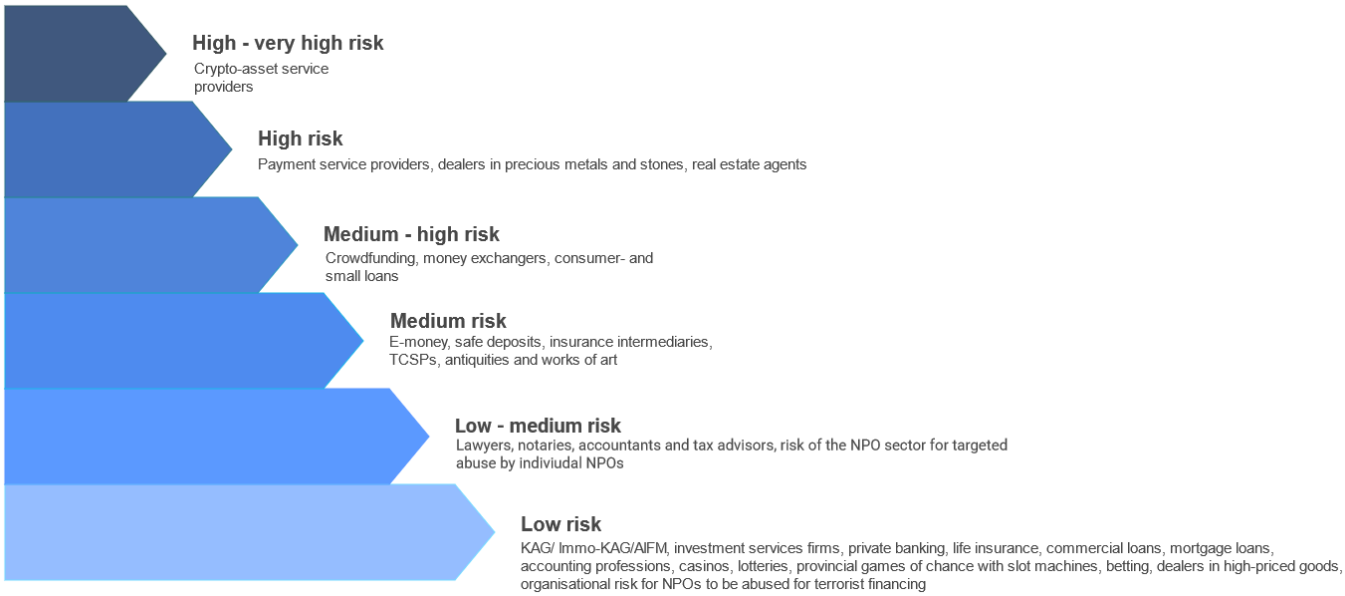
Intensity of the threat from terrorist groups:

very high	high	medium	low
	ISKP	IS	Al-Qaida
	Muslim Brotherhood		Takfirists
	North Caucasian groupings		

In Austria, legal sources of financing or the use of funds for terrorist organisations and individuals such as donations (collections), earned income, social welfare etc. are used. Fundraising through criminal offences (robbery, theft, fraud, etc.) has not been identified to date. Funds for small groups or individuals who took part in the jihad in Syria/Iraq or attempted to do so are usually raised from their own resources and from family and friends. The attack on 2 November 2020 and the preparations for attacks that have since been foiled were, according to available information, financed from the perpetrators' assets in line with a Lone Wolf perpetrator profile.

Due to the fact that there are large and active communities from relevant countries in Austria, which have lively association activity as well as financial connections to their home countries, the risk of terrorism financing is to be classified as **high**.

Sectoral risks:



1.3 Proliferation financing

Threat scenarios of proliferation financing:

very common	frequently	regularly	rare
financing the purchase of luxury goods for the DPRK regime	financing the acquisition of dual-use goods	financing the acquisition of proliferation-relevant goods	Raising funds to support a WMD programme
raising funds through foreign exchange for the DPRK regime	sanctions are violated intentionally or negligently		Financing the acquisition of services or technologies
concealment by legal entities (front companies, straw men)			

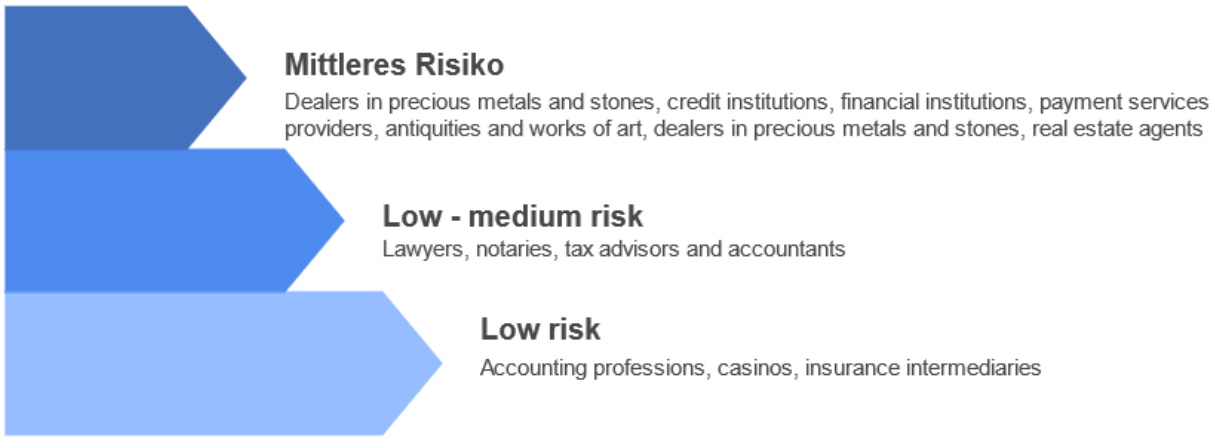
Methods of proliferation financing:

very high	high	medium	low
cash	bogus companies	cryptocurrencies	bank transfers
		hawala	

Austria is not only a transit country for proliferation-relevant goods, but also a target country for illegal procurement activities due to its highly developed industrial production and the large number of small and medium-sized enterprises, some of which are world leaders in certain areas. Dual-use goods, i.e. materials or products that can be used for both civilian and military purposes due to their technical specifications and high level of development, pose a particular problem.

Due to the fact that there are numerous companies in Austria that produce proliferation-relevant goods and the fact that state actors are willing to take covert measures to obtain these goods, the risk of proliferation-relevant activities and the linked necessary financing is classified as **medium.**

Sectoral risks:



2 Introduction

2.1 Objectives of the National Risk Assessment

The basis of all measures to prevent money laundering and terrorism financing taken by the authorities and obliged entities in the private sector is the **risk-based approach**. This requires a **comprehensive understanding** of the **national risk landscape**.

The aim of the National Risk Assessment is to create such a basis.

In accordance with article 3 (3) of the Financial Markets Anti-Money Laundering Act (FM-GwG) and **article 7 (4) of the 5th Money Laundering Directive (ML)**, the National Risk Assessment serves the following purposes:

- **Improving the system** to combat money laundering and terrorism financing, in particular to **identify any areas** where obliged entities need to apply **enhanced measures** and to **recommend the measures to be taken**.
- **Identification of sectors or areas** with a **low** or **increased risk** of money laundering and terrorism financing.
- **Identification** of money laundering and terrorism financing **risks** in relation to the development of **new products** and **new business practices**, including **new distribution mechanisms** and the use of **new or emerging technologies** for both **new** and **existing products**.
- **Allocation of resources** and **prioritisation** of resources for combating money laundering and terrorism financing.
- **Ensure** that appropriate regulations are established **for each sector or area** in line with the risks of money laundering and terrorism financing.
- Promptly **provide obliged entities with adequate information** to facilitate their own assessment of the risk of money laundering and terrorism financing.
- Reporting the **institutional structure** and **broad procedures of its own systems** for combating money laundering and terrorism financing, including in relation to FIUs, tax authorities and prosecutors, as well as allocated human and financial resources, to the extent that this information is available.
- Reporting of **national efforts and resources** (human and financial resources) made available to combat money laundering and terrorism financing.

- The Federal Ministers of Finance, of Constitutional Affairs, Reforms, Deregulation and Justice, of the Interior, of Digitalisation and Business Location, of Europe, Integration and Foreign Affairs as well as the FMA and the Austrian Central Bank must **take appropriate measures to achieve these purposes** within the scope of their responsibilities.

2.2 Preparation of the National Risk Assessment

The **2nd National Risk Assessment Austria (NRA II)** dates back to **2021**, since when the European and international legal framework has developed steadily. In addition, there has been a constant **development of the risk situation** and **the extension of the material laws** to new obliged entities. An update is therefore appropriate.

The starting point for the National Risk Assessment is the **National Coordination Committee for the Development of Measures and Strategies for the Prevention of Money Laundering and Terrorism Financing**, which has been established at the Federal Ministry of Finance. This is made up of all relevant departments and authorities.

Pursuant to **article 3 para. 2 FM-GwG**, the coordinating body must prepare and continuously update a National Risk Assessment in order to develop measures and strategies for the prevention of money laundering and terrorism financing. **The National Risk Assessment is based on** the **contributions of the members,** which they must prepare within the scope of their respective responsibilities.

The drafting process took place in three stages.

1) Based on a **common template and methodology**, the members prepared an **initial draft of their sectoral risk assessments**. These are **summary documents** in which the conclusions and results of **detailed preliminary analyses** are presented.
2) The first drafts were sent to the **Federal Ministries of the Interior and Justice** for **comparison with operational findings**. At the same time, the relevant **representatives of the private sector** received the draft report and were given the possibility to comment.
3) **Taking into account the feedback from** the Federal Ministries of the Interior and Justice as well as the private sector, **the final drafts were prepared** and consolidated into one overall document.

2.3 Methodology

The **updated National Risk Assessment (NRA III)** is meant to take into account the recommendations of the FATF Country Report 2016 and the requirements of the 4th and 5th ML Directive.

The sectoral risk assessments are based on the **methodology of the Supranational Risk Assessment (SNRA)**, which is to be prepared by the European Commission in accordance with Art. 6 (1) of the 5th ML Directive. A comprehensive description of the underlying methodology can be found in the Staff Working Document (SWD) of the SNRA 2017, p. 233 ff.

The key points of this methodological approach are briefly outlined below. The **threat** and **vulnerability** for money laundering and terrorism financing are each **assigned a value** (**low/medium/high/very high**), which corresponds to the SNRA values 1-4 (lowly significant/moderately significant/significant/very significant). **The categorisation of threat and vulnerability** follows the description of the SWD 2017, p. 248 ff. Quantitative figures and knowledge gained from supervisory activities serve as the data basis. This is followed by a description of the existing risk minimisation measures.

The overall risk is calculated using the formula: **40% threat + 60% vulnerability - risk-reducing measures = overall risk.**

Like the SNRA methodology, the National Risk Assessment assumes that **vulnerability** has **a stronger influence on overall risk** than threat and should therefore be weighted more heavily.

Finally, the sectoral risk assessments derive **recommendations** from the findings. As the National Risk Assessment is an authority document, it is only addressed to **authorities**. The competent authorities remain free to formulate further measures in relation to their obliged entities on the basis of the findings obtained as part of their supervisory activities.

3 Money laundering threat scenarios

Introduction

General description and database

3.1 The concept of "predicate offence"

This section examines the offence of money laundering (article 165 of the Criminal Code) from the perspective of predicate offences that are suitable for money laundering and presents - based on several sources - those predicate offences that are particularly frequently associated with money laundering and whose risk of commission is therefore high.

Pursuant to article 165 (1) StGB, the following shall be punished with imprisonment of up to five years

- anyone who either converts or transfers assets derived from certain serious criminal offences in order to conceal the illegal origin of the assets or to assist the offender in evading prosecution, or
- anyone who conceals or disguises the true nature, origin or location of assets derived from certain serious criminal offences.

According to article 165(2) of the Criminal Code, anyone who merely acquires, possesses, converts or transfers to another person assets which they know to be derived from certain criminal offences is liable to prosecution.

All these forms of money laundering are based on the fact that the assets to be laundered originate from certain criminal offences, the so-called "predicate offences". Not every asset is therefore suitable for money laundering. Money laundering is only possible if the assets in question originate from criminal offences punishable by more than one year's imprisonment or from articles 223, 229, 289, 293, 295 of the Criminal Code or articles 27 or 30 of the Narcotics Act. This condition of the predicate offence makes money laundering a so-called accessory offence.

Incidentally, for the purposes of criminal liability under paragraph 1, it is irrelevant whether the money laundering is committed by the same perpetrators as the upstream offence (so-called own money laundering) or whether it is committed by third parties (so-called third-party money laundering). Anyone who attempts to conceal the illegal origin of their own illicit funds through complex transactions via their own accounts may also be liable to prosecution for money laundering.

Finally, anyone who knowingly obtains, holds, invests or manages assets that are subject to the control of a criminal organisation or a terrorist group is also liable to prosecution under article 165(3) StGB. Due to the high criminal energy of such groups and the dangers they pose, the existence of a predicate offence suitable for money laundering is not relevant for this type of offence.

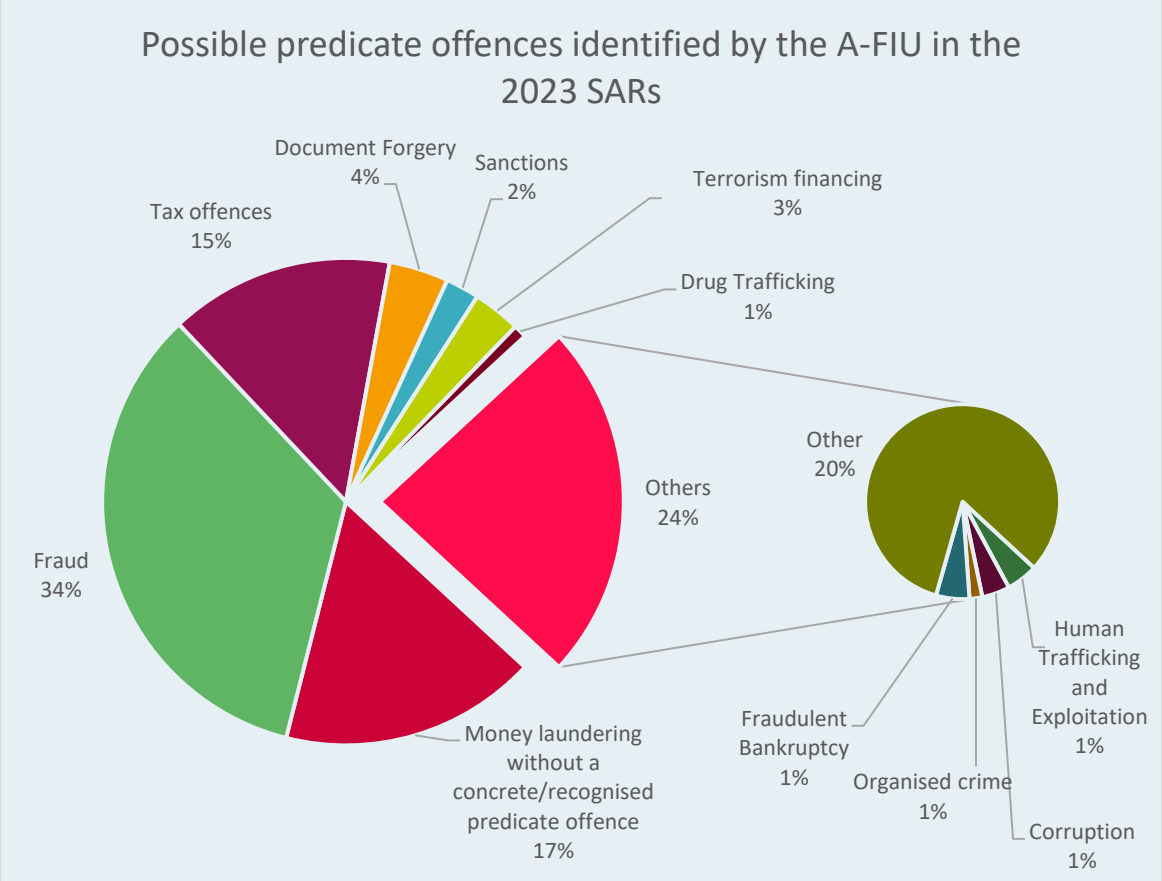
In Austria, money laundering is punishable under article 165 StGB regardless of where the predicate offence was committed. This means that, in principle, international offences can also be recognised as predicate offences to money laundering in Austria.

3.2 Data basis for the risk assessment

a)

The A-FIU is part of the security authorities and therefore bases the following analysis on the following sources: Firstly, as the central Financial Intelligence Unit, the A-FIU receives **suspicious activity reports** from the professional groups subject to reporting requirements and can derive the risk of their commission from the facts presented therein, which indicate certain predicate offences (Figure 1).

Graphic 1

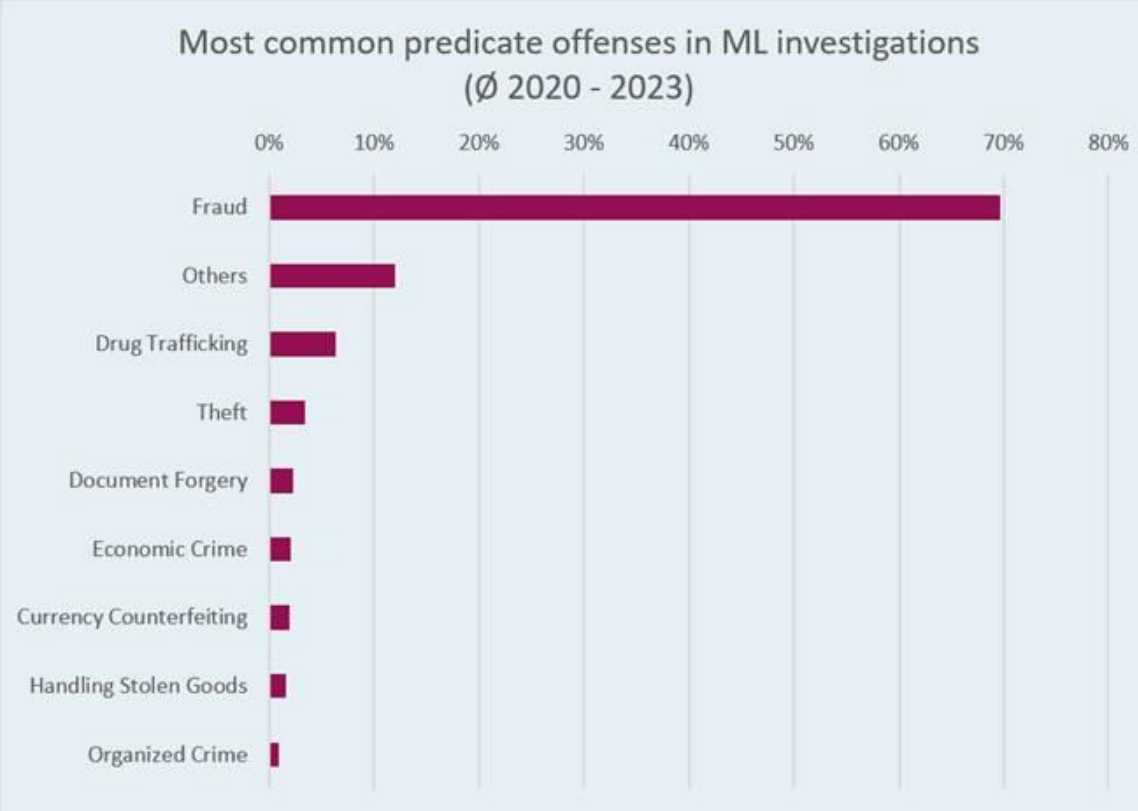


b)

Secondly, the analysis is based on data from the **crime statistics** of the general criminal investigation department from 2020 to 2023 (Figure 2). This makes it possible to determine the offences that were most frequently investigated (not convicted!) in connection with the basic offence of money laundering. However, it does not show those predicate offences that are investigated by specialised investigative authorities, such as the Federal Bureau of Anti-Corruption, the Directorate of State Security and Intelligence or the federal tax authorities.

The most frequent predicate offences shown in Figure 2 originate from 2,710 money laundering files that can be seen in the criminal police logging system in the period from 2020 to 2023.

Graphic 2



c)

The following analysis also takes into account predicate offences for which the A-FIU receives hardly any suspicious activity reports from reportable professions, but which are frequently **investigated by law enforcement authorities.** These are, for example, drug-related offences in which lower charges play a role and which are usually processed without the use of services from professions with reporting obligations.

A comprehensive description of predicate offences to money laundering can be found in chapter 9 of the Money Laundering 2023 management report.

How is incriminated money obtained? Predicate offences

Frequency of the predicate offence:

Very common	frequently	regularly	rare
Fraudulent offences	offences related to documents	Tax predicate offences	Organised crime
		Smuggling	Human trafficking/ Smuggling
		Social benefit fraud	Sanction violations
		Drug-related crime	Corruption

Very frequent predicate offences:

Fraudulent offences

According to police crime statistics, in the past three years, around 70% of investigations into money laundering were assumed to involve a predicate offence in the area of fraud.

The high frequency of fraud offences as a predicate offence to money laundering is also consistent with the findings that the A-FIU derives from the suspicious activity reports it receives, as suspicious activity reports on money laundering are most frequently filed on suspicion of fraudulent activities: Financial and credit institutions have long experience with this criminal phenomenon and therefore recognise the modus operandi that suggests fraudulent activities. In addition, many suspicious activity reports are made due to a callback from another bank whose customers recognise that they have been defrauded.

Fraud now mainly takes place on the internet. Due to the democratisation of the internet, almost everyone now has internet access and more and more areas of daily life are taking place online; the risk of becoming a victim of internet fraud is therefore correspondingly high. Based on the suspicious activity reports submitted to the A-FIU, goods delivery fraud, investment fraud or damage to assets by means of fraudulently obtained account data used to divert the victim's funds are particularly common.

The scams described are often due to the carelessness of the victims, but there is an increasing number of methods that can deceive experienced people. Fraudulent calls (spoofing) with Austrian numbers from abroad were prevented by an amendment to the Telecommunications Act 2024. This forces the perpetrator groups to operate their call centres in Austria, making them more accessible to Austrian authorities.

Frequent predicate offences:

Offences related to documents

Both the police crime statistics and the suspicious activity reports received by the A-FIU show the frequency of predicate offences in the area of document forgery. Between 2020 and 2023, an average of 2% of investigations into money laundering involved predicate offences in the area of

forged documents. In 2023, the A-FIU identified possible document offences as predicate offences in around 4% of suspicious activity reports.

Forged documents are particularly common in connection with the online opening of bank accounts using the video identification procedure or the qualified electronic signature. These procedures offer a large attack surface for AI technologies. Criminals have a major advantage if they are already in possession of stolen proof of identity, which can be fed to the AI in order to fake video sequences of the ID holder. In addition to banking transactions, mobile phone contracts can also be concluded in this way. Depending on the quality of the identification service providers used, the online identification procedure is easier or more difficult to outwit. Previous cases clearly show that criminals who open bank accounts with AI-generated false identities use them to receive and transfer fraudulently obtained funds. The problem is further exacerbated by the fact that, once "identified", bank accounts can easily be used to open additional accounts at other banks by means of SEPA verification (1 cent transfer).

Regular predicate offences:

Tax predicate offences

Financial offences can be considered predicate offences to money laundering if they meet the requirements of the money laundering regulations. A financial offence is considered a predicate offence to money laundering if
the value of the offence exceeds EUR 150,000 and there is intent.

In 2023, 15% of the suspicious transaction reports received by the A-FIU were classified as tax evasion offences (mainly bogus companies). The Federal Ministry of Finance publishes a list of the bogus companies identified on its website.

The conviction figures also show that predicate offences under financial criminal law are a constant threat. Tax evasion as a money laundering offence occurs primarily in connection with bogus company-constructs in the construction and service industries. The bogus companies are used to withhold social security contributions on a large scale and to evade taxes.

Example: Cleaning company, security

Cleaning companies that do not comply with the law can be recognised by various signs. These include the lack of a business registration, incomplete or incorrect certifications such as ISO 9001, and the absence of business liability insurance. Other indicators are the non-payment of social security contributions, working without bank processing, bogus self-employment or employing undeclared labour.

Indications may also include unusually low prices, non-transparent invoices (e.g. no detailed

service description or the absence of a VAT number) and the lack of safety clothing or tested chemicals. High employee turnover, incomplete homepage information or the lack of an imprint also indicate irregularities. In addition, invoices are often paid in cash.

If an execution title exists against an Austrian company (arrears with issued notices, enforcement order, seizure order), an execution can be carried out in accordance with Directive 2010/24/EU on assistance in the recovery of claims relating to taxes in other Member States.

Predicate offences in the customs area

In practice, there are three main groups of predicate offences to money laundering, namely under-invoicing, over-invoicing and smuggling.

Over-invoicing is a payment above the true value of the goods in order to generate money for corruption or breach of trust and consequently illicit money. The generation of money in connection with a predicate offence (e.g. corruption or breach of trust) will then be put into circulation as part of money laundering.

Smuggling

It takes place particularly in the area of excise taxes on cigarettes, mineral oil products, counterfeit medicines and drugs.

Underinvoicing

Under-invoicing of imported goods occurs in various customs procedures where import VAT is not collected during customs clearance and the goods are delivered to other EU countries after customs clearance. There is a risk that the recipient in the country of destination is a missing trader or that deliveries are made to missing traders via company networks and VAT is not collected (VAT carousel fraud).

There is a threat of fraud in the procedure with code 42xx. This customs procedure offers the advantage for honest traders that the import VAT is not collected at the time of customs clearance. On the other hand, this customs procedure harbours high risks for customs and tax administrations in the Member States (MS) of the European Union. For example, under-invoiced invoices are submitted for customs clearance in the importing country, some of which only show 10% of the actual value of the goods. Numerous inspections have also revealed excess quantities compared to the information in the freight documents. This results in massive reductions in customs duties in Austria and throughout Europe. In addition, in many cases VAT is not paid in the country of destination, the invoice recipients often do not exist (so-called "missing traders") and the goods are sometimes diverted to other countries. Some of the goods end up on European black markets or enter the legal trade after they have been made cheaper by the aforementioned fraud method. Diversion scenarios via other member states have also been observed. This risk also exists in the normal customs procedure, as the recipient can make use of his right not to pay the import VAT in the course of customs clearance under certain circumstances in accordance

with article 26 (3) Z2 UStG. The effect is the same as with customs procedure 42, the goods are in the internal market duty paid, the import VAT has not been paid.

Due to the high excise duty burden, cigarette smuggling is a particularly lucrative predicate offence. In 2023, a total of 1,416,753 cigarettes and 1,875 kg of excisable tobacco were confiscated in 1,950 cases.

Social benefit fraud

Social security benefit fraud is considered a predicate offence to money laundering if the assets obtained through the fraud are later "laundered" by concealing their origin or by integrating them into the legal financial cycle.

Social benefit fraud is defined as the unlawful claiming of social benefits by providing false information or concealing facts.

Social benefit fraud becomes a predicate offence to money laundering if the illegally obtained social security benefits (e.g. unemployment benefits, poverty relief assistance, minimum benefits) are later concealed through actions.

In such cases, the institution or authority that pays the social benefit in question is directly aggrieved. The state (e.g. unemployment benefit, family allowance), the social insurance institution (e.g. health, accident or pension insurance) or another public body may be the aggrieved party. As the Austrian state suffers a financial loss as a result of the predicate offence, only national predicate offences exist here.

According to the report of the 2023 Social Benefits Fraud Task Force, 18,700 reports with more than 20,000 suspects have been solved since 2018. Social benefit fraud is a "permanent fraud": If the fraud is not detected, the unlawful enrichment continues permanently. This is why the "prevented" damage is a central point in this special offence. Through targeted control and investigation measures, the Federal Ministry of the Interior’s task force on social benefit fraud was able to identify or prevent a total loss of more than 112.3 million euros from 2018 to 2023, with a peak of around 25.5 million euros being reached in 2023 (+80.7 per cent compared to 2022). This sum relates to both the actual loss incurred and the prevented loss. At 99.6 per cent, the detection rate is extremely high. Around 70 to 80 per cent of known cases involve people with foreign citizenship who are resident in Austria. The breakdown for 2023 is as follows: 1,250 suspects with Austrian citizenship, 3,394 suspects with non-Austrian citizenship. The most common nationalities of the accused in 2023 are Syria, Afghanistan and Ukraine.

Utilisation of social security benefits for investments

Example: A person who illegally receives a guaranteed minimum income or unemployment benefits by providing false information uses this money to buy expensive assets (e.g. a car, luxury goods, cryptocurrencies).

Money laundering: By purchasing goods or investing in cryptocurrencies, the origin of the money is disguised, as it is difficult to later trace that the assets originate from social security benefit fraud.

Drug-related crime

Offences against the Narcotics Act often occur in connection with money laundering investigations. Police crime statistics for the last three years show an average of 6% of money laundering cases, which were also investigated for illicit drug trafficking under article 27 of the Narcotics Act (SMG) and for the preparation of drug trafficking under article 28 of the SMG.

The frequency of offences and the associated risk are due, among other things, to the widespread use of addictive substances and their relatively high availability. The frequency of offences is reflected in the suspicious activity reports received by the A-FIU.

The purchase and trafficking of narcotics can be traced particularly frequently when analysing crypto transactions because purchases of narcotics are not usually processed via traditional bank transactions. Therefore, all suspicious activity reports received in this regard originate from crypto exchangers. In future, suspicious facts that suggest possible drug purchases will be forwarded directly to the competent investigating authorities if there are no indications of money laundering. The suspicious activity reports received indicate that these are usually national predicate offences (ordering drugs for personal use).

Rare predicate offences:

Organised crime

A special form of money laundering is committed by anyone who knowingly obtains, holds, invests, manages etc. assets that are subject to the power of disposal of a criminal organisation or terrorist group (article 165 para. 3 StGB); a specific predicate offence is not relevant here. Police crime statistics from the past three years show that, on average, 1% of money laundering investigations each year involved suspected assets belonging to criminal organisations.

Despite these low figures, the high criminal energy of such groups and the dangers they pose mean that the risk is high.

The fact that hardly any suspicious activity reports received by the A-FIU justify relates to a criminal organisation is because the connection between the transaction and a specific type or degree of organisation – unlike a specific predicate offence – is even more difficult to identify. Organised crime usually operates across borders.

Corruption

The available figures from SARs do not show a systematic threat of corruption. Suspicious activity reports from obliged entities are submitted in particular in connection with media coverage (adverse media reporting).

Sanction violations

Suspicious activity reports due to possible sanction violations led to a higher volume of suspicious activity reports from 2022 onwards, demonstrating a higher level of awareness in the obliged entity sector. Based on the figures available, the threat can be categorised as low overall.

How is incriminated money laundered? Methods

Very high	high	medium	Low
bogus companies	Offshore	Life insurance	
Fraudulent crime	Virtual currencies and cryptoassets	Online accounts	
	Luxury goods		
	Real estate		
	Prepaid cards		
	Hawala		

Very high threat:

Bogus companies

Bogus companies are companies that are officially registered but often do not carry out any actual business activities. They are usually set up for fraudulent or illegal motives. These companies often only exist on paper and are used to conceal their true purpose or actual economic activities.

Bogus company constructs occur primarily in the construction and service industries. The bogus companies are used to withhold social security contributions on a large scale and evade taxes.

The primary aim of the multi-level bogus company structures is to smuggle assets out of companies in order to make a profit and thus reduce taxes, so that they can then pay undeclared labourers in cash - again without paying taxes or social security contributions.

To this end, numerous limited liability companies are founded or taken over as shell companies. Only straw men act as managers who have nothing to do with the actual operational business of the company, so the actual beneficial owners remain in the dark. These dummy companies are linked in a chain and issue "invoices" to the respective upstream company for services that they have never actually provided. In this way, the upstream company has the necessary documentation to be able to include the profit-reducing outgoing payments in its accounts. The further down the chain a bogus company is, the shorter-lived it is and the fewer responsible parties can be found. At the end of the chain, the transferred funds are collected in cash and then kicked back to the top companies, which use them to pay the black wages.

The suspicious activity reports in this area of offence give an idea of the enormous dimensions of withheld social benefits and evaded taxes: In 2022 alone, bogus companies withdrew over 600

million euros in cash from their bank accounts. Money that is mostly used to pay undeclared workers and for which those involved pay neither social security contributions nor taxes. The suspicious activity reports indicate a high number of unreported cases. It can therefore be assumed that the actual volume of cash withdrawals amounts to around one billion euros, resulting in the evasion of payroll taxes, social security contributions, income taxes and, in some cases, VAT in the same amount.

As of 1 January 2025, 253 bogus companies based abroad are known in Austria because they have a connection to Austria (labour leasing). 901 bogus companies based in Austria were identified by official decision.

The funds generated in this way are often transferred abroad to make it more difficult for the Austrian authorities to access them.

Money laundering:

Bogus companies are used to conceal the trail of money movements. The illegal money is declared as "income" of the bogus company. After being booked as "profit" or "income", the money can then be used as legal money.

One of the most common methods of money laundering is the use of fictitious invoices. The bogus company issues fictitious invoices to real companies or other bogus companies. These invoices are formally correct but are based on services or deliveries that have never been provided. The money is then "laundered" by paying these invoices.

In another method (layering), money laundering takes place in several layers. Bogus companies often serve as one of the intermediaries to forward the money. This can be done through transfers to other companies, offshore accounts or investments in property or cryptocurrencies.

Bogus companies are also often founded in tax havens or countries with weak financial supervision. The true owners remain anonymous and there is no obligation to make annual reports or tax returns publicly available.

In the summarised scenarios of the Supranational Risk Assessment, the vulnerability of bogus companies with regard to abuse for money laundering purposes was classified as very high.

<u>Fraudulent crimes</u>

Investment and CEO fraud:

In CEO fraud, the perpetrators induce companies to make payments to certain accounts by pretending to be a leading employee and by building up time pressure. The authoritarian and well-planned (social engineering) behaviour allows employees to be deceived and they instruct corresponding transactions. These, in turn, have to be laundered through acts of concealment, in particular through frequent onward transfers to a large number of countries.

In the area of investment fraud, victims are often informed or made aware of supposedly lucrative investment opportunities (especially in digital currencies) via messenger services. If the victim then registers on the advertised platform, they receive a call from the "broker". High profits or opportunities for such profits are feigned. However, the investments made are never invested in real assets, but are forwarded directly to the money laundering system. Mention should also be made of the current phenomenon of "pig butchering", which initially begins at the level of a "love scam", usually via social media contact or a dating platform, and then turns out to be an enticement to invest money in fraudulent investment schemes. The perpetrators pretend to have amassed a large fortune through the same investment, which is also presented as a deception (e.g. through luxury cars). Through recurring payments by the victim, the victim is gradually financially excluded or "cannibalised". This fraud model - also known as business email compromise - is an international phenomenon. The fraudsters are often based in countries with weak law enforcement measures.

Money laundering:
Funds from fraudulent activities must always be transferred across borders from the address received as quickly as possible in order to avoid recovery by the victim's bank or to make seizure by law enforcement more difficult. The type of currency can also be changed, e.g. FIAT to cryptocurrency and/or vice versa, as well as the change from one cryptocurrency to another, including the use of so-called mixers or tumblers, in order to strengthen the concealment.

In the area of investment fraud, the phenomenon of "pig butchering" can be observed in particular. The victim is convinced to invest their money in a "legitimate" crypto exchange that the perpetrator recommends based on its merits. The website, wallet creation and other features look reputable and are often well-made copies of legitimate sites. Ignorance of the cryptocurrency market and the combination of romantic communication and initial fake successes prompt victims to invest more and more money. The money is deposited into digital wallets, trading platforms or the fraudsters' investment accounts. In reality, however, the funds are split up and transferred to a large number of addresses in the blockchain until they leave it. As a rule, the funds are sent to a distant foreign country after several splits and transactions, where they are rectified and reintroduced into the economic cycle elsewhere.

High threat:

Virtual currencies and cryptoassets
The general challenges with cryptocurrencies remain the time-consuming tracking of cash flows, the use of mixing services or the disbursement of funds by dubious exchangers based in uncooperative or weakly regulated countries. The attractiveness of cryptocurrencies for fraud and money laundering remains unchanged. Criminals take advantage of the highly complex technology and the victims' lack of expertise, coupled with the possibility of quickly removing the funds from the authorities' grasp.

The methods for money laundering are widespread in the cryptocurrency sector due to the existing pseudonymity and rapid processing. Time and again, it is noticeable that the use of stablecoins in particular is often used for fraudulent activities. Stablecoins are virtual currencies whose value is linked to an anchor value, such as a fiat currency, often the euro or US dollar. The aim of stablecoins is to avoid the typical high volatility while retaining the advantages of cryptocurrencies. Due to their stability, stablecoins are particularly popular with fraudsters, as the incriminated assets are only subject to a low volatility risk.

A popular method of money laundering in the crypto sector is the "peel chain". This is a technique used to launder large sums of incriminated money by means of a long series of micro-transactions. In each step, a small amount is "peeled off" and at the end the money is returned to (often different) crypto exchangers. Crypto exchangers that operate in countries with low regulatory intensity or decentralised platforms are often used for this purpose. Decentralised solutions (DeFi) are based on smart contracts, which means that products based on them are not subject to the control of a company and can run without the intervention of an intermediary (e.g. exchange/broker or bank). In the area of decentralised exchanges, stablecoins such as Tether (USDT) are primarily traded. This is one of the most widespread coins and is now part of most trading pairs.

The crypto market has a strong international character and is often cross-border. It can involve both national and international scenarios.

Offshore

The term "offshore" covers both traditional tax havens and jurisdictions that systematically allow low tax burdens (15% or less direct tax) or tax concessions (in principle or for a limited period). They also allow the client a high degree of anonymity.

Offshore structures serve the following purposes: no or low taxes in the destinations concerned combined with a high degree of confidentiality due to strict banking secrecy as well as secrecy regarding the identity of the beneficial owner and the transactions and the impossibility of exchanging information due to the lack of administrative assistance or mutual legal assistance agreements.

Even if agreements have been concluded, no substantive information is transmitted, as economic activity in the respective territory is prohibited.

Countries with strong banking secrecy include:

- Switzerland
- Singapore
- Hong Kong
- Seychelles
- Panama
- Belize

- Cayman Islands
- Maldives

Offshore structures are a key indicator of money laundering. Offshore leaks (e.g. PANAMA papers, LUX leaks, etc.) have revealed a large number of criminal offences that were made possible by offshore jurisdictions. Offshore structures are not only used for tax evasion, but also for committing a variety of criminal offences, such as fraud, fraudulent crida, breach of trust, but also for malpractices in office (corruption/bribery).

The following threat scenarios were observed in Austria:

1
An offshore company opens an account in Austria. Incoming foreign payments from actually operating companies and offshore companies are paid into this account. The accumulated account balances are settled in cash or transferred onwards (layering by legal entities). There are hardly any domestic investigation approaches, as the underlying transaction is not processed in Austria. Furthermore, it is almost impossible to determine who the actual beneficial owner of the company is. Foreign nationals are authorised. It is reasonable to assume that money laundering is carried out via such constructions.

2:
An offshore company has a domestic business address and/or a domestic bank account. Administrative activities - "mailings", "invoicing", "telephone forwarding", "payment instructions", etc. - are carried out from the domestic business address. From a criminal investigation perspective, there are hardly any domestic investigation approaches, as the underlying transaction is not carried out in Austria and it is unknown who the actual beneficial owner of the offshore parent company is. This results in enormous account turnovers, the information - assuming it is available - is not meaningful and does not allow criminal investigations to be initiated. It is reasonable to assume that money laundering is being carried out via such structures.

3:
An Austrian legal entity is a subsidiary of a foreign offshore company. It was founded by a foreign trustee and can be administered both from Austria and from abroad. If goods are delivered, these are only invoiced via Austria - without VAT - but the payments often relate to "intellectual services" such as feasibility studies, consultancy agreements, etc. This results in enormous account transactions. Austrian nationals act as managing directors, board members or shareholders. The legal entities have identical company addresses. They issue bogus invoices for fictitious underlying transactions. It is reasonable to assume that money laundering is being carried out via such constructions.

Luxury goods

Especially in the final phase of money laundering, the reintegration into the economic cycle, "whitewashed" incriminated assets, which now give the appearance of a legal origin, are well suited for the purchase of luxury goods such as jewellery or high-priced designer goods. Here, traders can be misused for money laundering purposes. These items are of particular interest to criminals due to their stable value. The luxury goods sector in particular (watches, handbags, etc.) even enables significant value gains to be made on sale. However, tradespersons can also play an often involuntary role in the earlier stages of the money laundering process. This is done by not complying with money laundering prevention rules and thus enabling concealment activities, e.g. by purchasing incriminated jewellery. In this case, the application of money laundering prevention regulations can prevent the transaction in advance. A great deal can also be achieved preventatively through increased monitoring by the supervisory authorities.

These can be both national and international scenarios.

Real estate

Property plays an important role for money launderers internationally, but of course also in Austria. The property market in Austria in particular is known for its stable value as well as its potential to increase in value. In addition, large assets can be invested and property offers good explanations for a high use of funds. In practice, there are a variety of methods for laundering money by means of a property purchase. A property acquisition usually has points of contact with various obliged entities. On the one hand, lawyers, notaries and estate agents are involved and, on the other, banks that handle the property transaction. There is therefore a great deal of potential for preventing money laundering before the transaction is finalised.

The predicate offences can be both national and international. In the case of foreign nationals, the predicate offence is usually committed abroad.

What can such a money laundering process look like?

Domestic or foreign legal entities are used as the buyer of the property. These are often incorporated into a network of companies with links to offshore destinations. Incriminated money, which is channelled through these networks and often passed on to the purchasing company by means of a loan agreement, can be invested here. The loan agreement is cited as proof of the origin of the funds. Countries with weaker control mechanisms are specifically chosen as the destination for the company headquarters. The purchase of existing shelf companies in Austria also plays a recurring role in this context. Other variants for using a property for money laundering purposes include undervaluing or overvaluing it. For example, an undervaluation can result in the price agreed in the purchase contract being below the actual market value. However, the difference to the actual value is paid in cash under the table. This, in turn, offers money launderers opportunities to invest and thus launder incriminated funds.

Prepaid cards

Prepaid cards - especially prepaid credit cards - offer a high degree of anonymity. On the one hand, such cards can be purchased online or at tobacconists or supermarkets without much effort. On the other hand, "vouchers" or a cash deposit at partner businesses such as various tobacconists can be used to top up these cards, which can also be used without legitimisation or verification of the origin of the funds. However, there are limits for these cards, depending on the respective provider. Some providers even allow you to send money.
The money laundering activity involves the easy transfer of cash to cards for the purpose of topping them up. This can then be used to invest incriminated money in the purchase of items using card payments or to send it abroad without the need for a local bank account. The cards can also be easily passed on anonymously across borders with the corresponding PIN code, as a cardholder never emerges from these cards. The funds usually originate from petty crime/street crime (e.g. theft, drug sales). These predicate offences are usually committed in Austria.

An additional act of concealment can make it particularly difficult to trace the illegitimate origin of the money. An example of this would be the use of (often fraudulently obtained) prepaid credit cards in the casino to exchange the incriminated funds for gambling chips. The subsequent conversion back into cash in turn offers an additional opportunity to conceal or prove the origin of the funds and thus also makes it more difficult to trace the incriminated assets.

Prepaid credit cards can therefore be used in a variety of ways for money laundering purposes and are therefore also associated with a high risk.

Hawala
Hawala is a globally widespread and functioning informal transaction system that exists in parallel to conventional banking. However, it first became widely known after the terrorist attack in the USA in 2001. At that time, investigators made it clear that HAWALA was the financial pillar of these attacks.

The use of hawala-like systems to launder incriminated money remains a high risk. Often, such a construct can only be uncovered by chance during other investigative activities, as various commercial enterprises (e.g. jewellers, mobile phone shops, restaurants, money remitter shops) are used as a cover to carry out hawala transactions in the background. In connection with such money transfer systems, evidence has repeatedly been found that they are used to finance illegal activities. In particular, there have been links to human trafficking, drug trafficking and terrorism financing. Tracing is made more difficult by the use of such a system, as the identity of the sender or recipient is difficult to establish and regulated countermeasures are deliberately circumvented. In principle, the transaction takes place between a money sender, two corresponding hawaladars and a money recipient who gives the payer a code word and the amount.
In most cases, such transactions can only be traced through the closely guarded books of the respective hawaladar.

Medium threat:

Life insurance

In the area of life insurance, high single payments are particularly suitable for money laundering purposes.
By cancelling the life insurance policy - albeit at an uneconomical surrender value - the policyholders not only obtain their assets quickly, the payout by an insurance company also gives the impression of a legitimate source of funds.

Withdrawals from a life insurance policy offers the following advantages:
A large amount of incriminated funds is invested immediately and is no longer visible. This can even remain parked inconspicuously until the statute of limitations for criminal prosecution expires. The identity of the beneficial owners is only known to the insurance company, as life insurance policies are not entered in any special register.
International experience also shows that transaction monitoring for life insurance policies with single premiums is only effective to a limited extent, especially if there were no indications of a criminal origin of the assets at the time of payment. A re-examination of the individuals involved for indications of money laundering and their predicate offences is usually only carried out when a claim is made.

Other ways of misusing life insurance for money laundering purposes, also in combination, include taking out loans. The necessary collateral for the loan is then provided by a life insurance policy. The assets paid out as part of the loan originate from a bona fide source that is not scrutinised further. If an - unintentional or intentional - loan default subsequently occurs, the creditor bank will have no particular interest in scrutinising the outstanding life insurance policy.

There is no clear pattern, but they tend to be national scenarios.

<u>Online accounts</u>
Accounts that can be opened without identification at a physical branch have proven to be a common means of money laundering activities in recent years, or of initially receiving and then transferring funds from predicate offences. The popularity can be explained quite simply. On the one hand, it can be opened from anywhere in the world; a specific location is often not necessary. Secondly, the systems for online verification are often quite easy to fool. Of course, this depends on the quality of the provider in question and the verification package selected. Poor products on the market can be fooled very easily, even without using an AI in the background. However, the use of AI systems offers a wide range of possibilities, especially in the area of online verification. One major advantage for criminals, for example, is if they are already in possession of stolen proof of identity, which can be fed to the AI in order to fake video sequences of the ID holder.
Depending on the quality of the identification service providers used, the online identification process is easier or more difficult to trick using AI. However, previous cases show that criminals use the bank accounts that they open using AI with false identities to receive and transfer fraudulently obtained funds. The problem is further exacerbated by the fact that once a bank account has been "identified", further accounts can easily be opened at other banks using so-called SEPA verification (1 cent transfer).
The Europe-wide free instant bank transfer will further increase the relevance of such accounts for use in money laundering activities. In combination with a large number of bank accounts that can be opened (too) easily in false names, incriminated funds will be out of reach of the

investigating authorities long before the false identities are even recognised. At this stage, the money has already been transferred to the next concealment operation and is often no longer recognisable as such.

Conclusion

Money laundering methods are undoubtedly diverse and numerous. The methods highlighted here have emerged in particular from analyses and procedures conducted by the A-FIU and the BMF. Incriminated funds must always be laundered, regardless of the respective predicate offence. The further development of technical possibilities also opens up new possibilities in the world of money laundering. For example, forms of virtual currencies or cryptoassets or the virtual IBAN have emerged that enable greater concealment of identities or minimise market value risks.

Other possibilities include infiltration into companies and the use of offshore constructs in the background. In the construction industry in particular, there have been perceptions for several years that company constructs are being used to pass on money by means of kickback payments and fictitious invoices, which are ultimately used to pay illegal wages in cash.

However, it should also be emphasised that there are other methods of money laundering that have received less attention to date and which are considered to be high risk. These include, in particular, the practice of investing incriminated funds in life insurance policies and misuse them for money laundering purposes. Especially as this allows large sums to be invested without being entered in a register accessible to the authorities. But familiar forms such as hawala and property have also come to stay.

4 Threat scenarios for terrorism financing

Introduction
Anyone who provides or collects assets with the intention that they will be used, even if only in part, to carry out ... terrorist offences ... (article 278d StGB). Assets are tangible, intangible, movable or immovable objects, regardless of how they were acquired, legally relevant documents or deeds (electronic/digital) that prove the right to assets or rights thereto, bank loans, traveller's cheques, bank cheques, money orders, shares, securities, bonds, bills of exchange, letters of credit, etc. (§ 278d StGB). The financing of terrorism is currently limited primarily to maintaining the organisation of terrorist groups. The upkeep of such a group, even if it is not located in a crisis area, requires financial resources for strategic tasks such as propaganda, recruitment of new members and to cover the organisational costs and living expenses of the cadres. Austria was the target of terrorist attacks in the 1970s and 1980s, but then developed into a transit and retreat country where financing, recruitment and propaganda were carried out. The terrorist attack on 2 November 2020, but also foiled plans for attacks such as the 2023 Rainbow Parade, New Year's Eve 2023 and the Taylor Swift concert in 2024, show that Austria is once again a target country for terrorism. As of 1 January 2024, there were 1,800,866 (or 19.7%) non-Austrian nationals living in Austria out of a total population of 9,158,750 compared to 1,146,078 (or 13.3%) on 1 January 2015. Of these, 877,853 were third-country nationals as at 1 January 2024 compared to 707,780 in 2020 and 566,000 in 2015. Around 32% of third-country nationals come from the Western Balkans. Approximately 14% are Turkish nationals. 95,180 or 10.8% come from Syria and 13,256 people (or 1.5%) from Iraq. 54,955 people (6.3%) come from the crisis region Afghanistan/Pakistan, 37,332 people (or 4.6%) are citizens of the Russian Federation, a large proportion of whom come from the North Caucasus. There are 80,665 Ukrainian citizens living in Austria, making up 9.2% of third-country nationals. All of these areas are or have been conflict regions in the recent past (Turkey, North Caucasus, former Yugoslavia, Afghanistan, Iraq and Syria) Since the early 2000s, there have been jihadi travellers or foreign terrorist fighters who first travelled to Afghanistan and from 2013, with the emergence of the so-called Islamic State (IS), to Syria and Iraq to join various groups there. These were converts, third-country nationals as well as Muslims born in Austria with Austrian citizenship. Over 300 people from Austria are said to have successfully left or attempted to do so. Following the military pushback of IS in Syria in 2019, this trend has declined sharply, but the idea is still being discussed in radicalised circles. At present, relatives and friends of these foreign terrorist fighters are keen to help their relatives or friends return or to free them from captivity. In the meantime, returnees from jihad pose an

undefined potential danger, as some have been reformed, while others hold on to their radical ideas.

On 7 October 2023, there were numerous coordinated attacks by Hamas in Israel in which 1180 people, including 797 civilians, were killed on the Israeli side and 251 people were taken hostage. This triggered a war between Israel and Hamas in the Gaza Strip. In Lebanon, where the terrorist organisation Hezbollah, which is allied with Hamas, has a strong presence, rocket attacks created a second front characterised by artillery battles. In Austria, there have been expressions of sympathy for Gaza since the beginning of the armed conflict, particularly in the Muslim community. There is a risk that the events and the suffering of the people in the Middle East will be used for radicalisation and recruitment, but also as a motive for fundraising, which in reality is used for terrorism financing.

Intensity of the threat from terrorist groups

Very high	high	medium	low
	ISKP	IS	Al-Qaida
	Muslim Brotherhood		Takfirists
	North Caucasian groupings		

High threat:

Islamic State Khorasan Province

The ISKP currently poses the greatest terrorist threat to Austria. The ISKP has established transnational networks that plan large-scale attacks in Europe. These networks endeavour to raise funds to finance terrorist activities and carry out attacks. Links to actors in Europe can also be identified.

Muslim Brotherhood

Members of the Muslim Brotherhood in Austria have access to far-reaching international networks, some of which have access to considerable sums of money. The Muslim Brotherhood raises funds in various ways, including donations, companies, international organisations and financiers: Donations, companies, international organisations and financiers. Officials and organisations close to the Muslim Brotherhood are regularly accused of financially supporting the terrorist organisation Hamas. This is said to involve the systematic misappropriation of donations collected under the pretence of humanitarian aid. Frequently, the money flows through supposed charitable organisations that transfer large sums to various countries abroad and from which parts are diverted to Hamas officials. In October 2024, for example, new sanctions were published by the US Treasury Department against a person living in Vienna who is allegedly involved in

financing Hamas. The person is a board member of several associations in Austria and at European level and has close links to alleged Hamas donation networks in Europe.

North Caucasian groupings
Chechen jihadist actors in Austria have in recent years taken on leading roles within transnational IS financing networks. In summer 2024, for example, house searches and arrests were carried out on eight men and one woman who were part of an IS financing network in Austria. All nine people were of Chechen descent. It is alleged that large sums of money were channelled to finance IS activities in Europe and to support IS supporters in Syrian refugee and detention camps.

Medium threat:

Islamic State
Within the Islamic State, as already mentioned, the Chechen financing networks and the structures of the ISKP pose the greatest threat in Europe. However, there are also other financial connections of IS supporters in Europe that are used to spread the ideology and finance terrorist activities. The Islamic State continues to endeavour to recruit in Europe and carry out attacks that attract media attention. There are often overlaps with the North Caucasian actors mentioned above and the networks of the ISKP.

Low threat:

Al-Qaida
Al-Qaeda is currently concentrating on mobilising individual perpetrators in Europe. At present, no Al-Qaeda financing networks with a wide reach and well-established structures can be identified in Austria.

Takfirists (Western Balkans)
Takfirism is a branch of jihadism whose followers are largely considered to be violent and particularly radical, as the enemy image of the infidels is particularly broad. Takfirist groups in Austria generally have no significant financial structures. They are generally financed by membership fees and donations.

How are funds generated for terrorism financing?

Terrorist organisations mainly collect money from their own community and are very clandestine in their approach. The more the donors can identify with the organisation's "cause", the easier it is to raise funds. Sympathisers of terrorist organisations often only have very limited financial resources. Nevertheless, it is known that considerable sums can sometimes be raised through fundraising. The money is collected through intermediaries, via unregulated crowdfunding platforms, but increasing international attention is also being paid to fundraising by non-profit organisations, the proceeds of which can be used for terrorism financing. The true purpose is (usually) unknown to many small donors. In addition, giving a donation is a commandment in

many religions and usually consists of small and very small amounts. In well-organised groups, (cultural) associations are run to cover the true purpose, whereby the cultural purpose of the association is placed in the foreground to the outside world.

How are funds transferred for terrorism financing?

Funds for terrorism financing are almost exclusively destined for third countries (Russian Federation, Turkey, Middle East, Somalia, Afghanistan, Pakistan, Iraq, Syria, Somalia, etc.), meaning that the final recipient country and the final recipient can hardly be reliably determined, as funds are sometimes also forwarded via other third countries. In addition, there is evidence of remittances from relatives or close associates of people who have travelled to crisis regions and who wish to join or have already joined the armed jihad, as well as those who are only on their way to these regions.

Due to its geographical location, Turkey continues to be a third country often used by terrorist groups and their sympathisers for financial transactions when jihadi travellers are to be supplied with funds. Furthermore, terrorist organisations targeting this state are active in Turkey, which means that Turkey is also a target country for transactions.

Funds are transferred to the destination country by official financial service providers (MVTS) and, if this is not opportune or possible, e.g. if there is no bank connection there, by unofficial agents (hawaladars). Any number of intermediaries can be used to disguise the final destination. Terrorist organisations generally use cash couriers when large sums need to be transferred in order to avoid the strict money laundering and terrorism financing requirements to which obliged entities are subject. On the other hand, transfers are made via a third country or through a correspondent bank located in another country if there is no direct banking connection to the destination country. However, these money transfer centres are used by many people for a wide variety of reasons (family support in the home country, trade, etc.).

Therefore, there can be no general suspicion regarding these transfers, as intermediaries are primarily used for personal reasons in addition to the argument of the lack of infrastructure in the crisis region. Apart from legal financial service providers such as banks and remittance service providers (Western Union, MoneyGram, Coinstar, etc.), trustworthy contact persons in the country of origin or destination are often entrusted with the transaction, even though this is usually not legally permissible due to the trusteeship assumed. These trusted contacts are usually co-nationals or at least people from the same cultural background.

Cash couriers can only be recorded by customs when entering and leaving EU territory, but this is now only possible in Austria at airports and at the border with Switzerland and Liechtenstein (§ 17b ZollR-DG).

Risk minimisation measures

Suspicious activity reports from banks and other obliged reporting entities are checked by the Financial Intelligence Unit with regard to the recognised reason for reporting. If there are grounds for suspicion regarding terrorism financing, these STRs are processed further by the Directorate of State Security and Intelligence. The fluctuation in the number of suspicious activity reports between years is striking. However, looking at the peaks in 2017 and 2021, it is clear that major attacks, such as the Christmas market in Berlin at the end of 2016 and the attack in Vienna on 2 November 2020, have raised awareness of the problem of terrorism financing. By August 2024, there had been 152 suspicious activity reports relating to terrorism financing. Extrapolated to the whole of 2024, this again results in a peak in the number of reports. This is again presumably due to the prevented attacks at the Rainbow Parade and New Year's Eve 2023 and the Hamas-Israel conflict, among other things.

Year	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Suspicious activity reports	113	148	203	167	93	113	204	155	212	233

In the vast majority of STRs, conspicuous customer behaviour and the matching of the name or parts of the name of the originator or recipient with names of persons or organisations on sanctions lists (EU, UN, OFAC, ...) are cited as the (main) reason by the financial service providers submitting the SARs. Furthermore, the amount of the transaction sums and the frequency of the transactions carried out are named as conspicuous. It is important that obliged entities always weigh up all the circumstances in addition to checking objective criteria such as name matches, sanctions lists or certain destinations (know your customer).

Individuals and organisations that use the services of a financial service provider for the purpose of terrorism financing are aware that their actions are subject to scrutiny, which is why it can generally be assumed that there is an (attempted) concealment of the actual use of funds, for example by pretending that the reason for the donation is not real. As soon as a money service provider switches to de-risking and blocks the customer account, further misuse of the account is prevented, but the possibility of further monitoring of the account movements is also removed.

The processing and analysis of suspicious activity reports by the Financial Investigation Unit and the Directorate for State Security and Intelligence is a primary way of minimising risk in addition to potential criminal prosecution. Possible developments and modi operandi can be recognised and discussed in the context of interministerial cooperation and exchange with reporting authorities in order to develop measures.

Conclusion and risk classification

In Austria, legal sources of financing or the use of funds for terrorist organisations and individuals are used, e.g. through donations (collections), income, welfare, etc. Fundraising through criminal offences

(robbery, theft, fraud, etc.) has not been identified to date. Funds for small groups or individuals who participated or attempted to participate in the jihad in Syria/Iraq are usually raised from their own resources and from family and friends. The attack on 2 November 2020 and the preparations for the attack that have since been foiled were, according to available information, financed from the perpetrators' assets in line with a lone wolf perpetrator profile.

Due to the fact that there are large and active communities from relevant countries in Austria, which have lively associations as well as financial connections to their home countries, the risk of terrorism financing is to be classified as **high**.

5 Threat scenarios for proliferation financing

Introduction
Definition: The term **proliferation** refers to the further spread of nuclear, biological and chemical weapons of mass destruction, the delivery systems required for them, and the products used to manufacture them, including the necessary expertise. Relevant processes are not limited to the proliferation of weapons of mass destruction, but also include projects aimed at completing existing arsenals of weapons of mass destruction, improving their storage capacity, usability and effectiveness, or developing entirely new systems. The illegal proliferation of dual-use goods to war zones and the illegal procurement of dual-use goods also falls under proliferation in the broader sense from an Austrian perspective. It should be noted that there is no standardised international definition of proliferation. Accordingly, **proliferation financing** is the financial facilitation of the proliferation of nuclear, biological and chemical weapons of mass destruction and the associated means mentioned in the first paragraph. **Tasks, legal basis and description:** The main tasks of combating proliferation are identifying relevant companies and procurement networks, uncovering concealed payment flows and clarifying whether and in what form state-initiated structures, such as foreign intelligence services, are involved in such activities. Proliferation-related activities are considered attacks that jeopardise the constitution and the Directorate State Protection and Intelligence Service (DSN) is tasked with combating them. The prevention of proliferation financing is also regulated in the FM-GwG, GewO, NO, RAO, GSpG, Accountancy Act and WTBG. Proliferation financing also includes the non-implementation and circumvention of targeted financial sanctions in connection with proliferation financing imposed in accordance with Decision (CFSP) 2016/849 and Decision (CFSP) 2010/413 as well as Regulation (EU) No. 2017/1509 and Regulation (EU) No. 267/2012. This applies in particular to the **Democratic People's Republic of Korea** (DPRK) and the **Islamic Republic of Iran**. The sanctions regime against the **Islamic Republic of Iran** (Regulation (EU) No. 267/2012 and Decision (CFSP) 2010/413) is characterised by the Vienna talks and the JCPoA. Resolution 2231 (2015) entering into force led to a noticeable easing of the situation between the signatory states, meaning that sanctions against Iran could subsequently be eased. In response to the withdrawal of US President Trump and the associated reintroduction of US sanctions, Iran continued to enrich uranium. Between 2021 and 2022, US President Biden made a new attempt to persuade Iran to return to the requirements of the JCPoA on the basis of negotiations, but this was unsuccessful.

This means that US sanctions and secondary sanctions as well as limited EU sanctions are still in place against Iran, although these mainly relate to proliferation-relevant goods.

The sanctions regime against the **Democratic People's Republic of Korea** is one of the most restrictive sanctions regimes and is based on UN Security Council resolutions. The DPRK has been researching and developing nuclear weapons and ballistic missiles for decades and has a large stockpile of chemical warfare agents. The rapid development of missiles, which can by now reach Europe, is a serious threat to the security of the EU and Austria. The sanctions regime affects large parts of North Korea's external presence. This means that far-reaching business areas of the DPRK are potentially subject to sanctions.

Current dynamics:
The increased global threat situation and the current international trouble spots, such as the Russian war of aggression against Ukraine and the Middle East conflict, are also increasing the threat situation in connection with proliferation and proliferation financing. In order to successfully prevent the procurement processes of international proliferation networks, cooperation between the DSN's proliferation defence and other competent national authorities is of paramount importance. Export control in the Federal Ministry of Labour and Economy and Austrian customs in the Federal Ministry of Finance play a central role in this. In the area of export control, weapons, military goods and dual-use goods are subject to a licence requirement. Under certain circumstances, this authorisation requirement may also be necessary for free goods that are not subject to any restrictions. The DSN is involved in the decision-making processes within the framework of export control.

Global risk landscape

Democratic People's Republic of Korea (DPRK):
North Korea has one of the most complex and at the same time most successful systems for circumventing sanctions. It also has an advanced nuclear weapons and missile programme. These weapons programmes are seen by the ruling regime as an essential component of maintaining power and shaping foreign policy and are therefore given the highest priority. The Asian country is one of the most heavily sanctioned countries in the world by the UN. Nevertheless, the regime is able to make immense progress in the further development of it´s weapons systems. The nuclear arsenal in North Korea is constantly changing, with around 30 nuclear weapons being assumed to date. Particularly in view of the constant tensions with its neighbouring states and the USA but also the recurring export of weapons or technologies and know-how to other states, North Korea's proliferation-relevant actions are a constant cause for concern.

The geopolitical developments of recent years see North Korea as one of the biggest beneficiaries of the newly strengthened East-West conflict. Trade with Russia is experiencing a strong upswing and China is interested in investing in North Korea. At the same time, the country benefits from not having to fear pressure from Russia or China due to its weapons of mass destruction

programmes. These two actors have lost interest in maintaining or monitoring compliance with the international sanctions regime against the DPRK.

The international sanctions resulting from the actions of the North Korean regime (continuous continuation of missile tests, expansion of the defence industry, threats to use its weapons arsenal and serious human rights violations) have meant that the country has been unable to meet its needs for foreign currency, materials, goods and technology from its own or legitimate economic activities for decades. A deep specialisation in illicit procurement networks for finance, materials and technology has led to the development of the most successful and enduring system for circumventing sanctions to date. The North Korean regime does not shy away from involving elements of organised crime either. The country has massively expanded its capabilities in the area of cybercrime in particular. The North Korean regime commissions the circumvention of sanctions and demands their implementation from nationals. It must be assumed that every North Korean person, group and entity is acting on behalf of the state. North Korean nationals can only travel abroad on state orders and passports are only issued to private individuals belonging to the elite class loyal to the regime for the fulfilment of special orders.

One of the North Korean regime's most lucrative sources of income is the export of weapons and armaments to non-state actors, such as al-Shabaab in Somalia or the Wagner mercenaries, as well as to state actors such as Iran, Syria and Russia.

For decades, Austria has been a relevant location for the coordination of sanctions evasion by intelligence service actors of the North Korean regime. The relevance of Austria as a location for North Korean activities currently appears to be increasing. This represents a problematic and challenging situation for Austria. While the North Korean regime appears to be reducing its presence globally, as recently demonstrated by the closure of numerous embassies and trade departments worldwide, this trend is not being recognised in Austria. In the eyes of North Korea, Austria is of great importance as a strategic and operational location for foreign activities. This circumstance has the potential to damage Austria's international reputation and political credibility.

Iran:
The Islamic Republic of Iran has been suspected of running a covert programme to produce nuclear weapons for years. Austria is also affected by Iran's arms programme. Its space programme is intended to provide knowledge for the development of long-range missiles capable of delivering nuclear warheads over many thousands of kilometres - and therefore also to Europe. As one of the most important European industrial nations and home to numerous high-tech companies, Austria is also of interest to the Iranian armaments programme. In the past, the attempted purchase of engines from an Austrian manufacturer via a Chinese company construction for Iran became known.

Russia:
Although this risk assessment is limited to Iran and North Korea, it is important to recognise that proliferation financing uses procurement strategies that rely on global networks. State and non-state actors knowingly or unknowingly contribute to proliferation networks and in some cases co-operate increasingly closely.

In recent years, the Russian war of aggression against Ukraine has become a key factor in the fight against proliferation. In the course of this, Russia has become increasingly associated with the proliferation financing efforts of the DPRK and Iran, so that it is no longer appropriate to analyse the two states without taking Russia into account. A military alliance was concluded with the DPRK, on the basis of which both weapons and soldiers from the DPRK are demonstrably being deployed in Ukraine. Iran supports Russia through the confirmed delivery of a large number of drones, whereby the demand for military drones on the Russian side remains as high as ever. The production of Russian attack drones has also been partly outsourced to Iran.

The development towards a war of attrition led to a high demand for military goods on the Russian side. In response to this, Russia has converted its own economy to a war economy in the medium term. In particular, the production of artillery shells, drones and ammunition is being driven forward in a resource-intensive manner. At this point, the phenomena of proliferation and the international illegal arms trade are merging.

As the Russian defence industry is affected by extensive EU sanctions, all available means are being used to circumvent them in order to meet its demand for military goods. The covertly procured goods are predominantly dual-use goods, which are procured using state and non-state actors while concealing the actual end users. Such procurement measures are also carried out with the involvement of the Russian intelligence services, which have a global presence. However, this modus operandi is not limited to the defence industry; other civilian sectors of the Russian economy, which want to obtain spare parts for machines, for example, also attempt to procure these - by circumventing the sanctions. The Russian intelligence services and third countries, which are considered Russia's strategic partners, are also used for this purpose

In Austria, opportunistic business people are among those recruited for proliferation-related activities. They often have roots in Russia or the republics of the former Soviet Union and usually set up several front companies in Austria. Exports from the EU are organised via these front companies. In Russia's "neutral" neighbouring countries, this creates a multi-layered, complex distribution network that is often difficult for the authorities to grasp. The target countries of Russian sanctions evasion in connection with proliferation are currently mainly Turkey, Kazakhstan, Kyrgyzstan, Uzbekistan, Armenia and, above all, China. In China, the supplier companies are often founded and operated directly by Russian businessmen or employees of Russian services. By acting as a middleman for key technologies, China is providing crucial support to Russia's war effort in Ukraine.

China:

China occupies a special position in global proliferation. While Russia concluded bilateral arms agreements with Iran and North Korea in 2023 particularly in the production of drones, China acted as a global buyer for sanctioned states on the European market as well as in Austria. Therefore China must also be taken into account in connection with the efforts to finance proliferation by the DPRK and Iran. In this context, North Korea, for example, is attempting to circumvent the provisions of Austrian export controls through a network of intermediaries in China. By providing a false - often civilian - end user in China, Austrian companies and the official export control authorities are deceived. Iran also frequently installs Chinese-made copies of Austrian products in drones which are ultimately delivered to Russia.

As Russia, for example, has no significant chip production, it is reliant on foreign countries. According to open sources, the country has managed to import sanctioned microchips worth more than 500 million US dollars via China and in particular via the Hong Kong Special Administrative Region. Customs data shows that some of the imported goods originate from the production of a German chip manufacturer, which also operates a subsidiary in Austria.

China is pursuing a dynamic export policy in sanctioned countries such as Russia. From this point of view, company takeovers in Austria by Chinese investors should also be scrutinised with great care. Particularly in the area of dual-use technologies, China is utilising goods originally developed for commercial use for military purposes. In this context, even supposedly harmless research co-operations or joint ventures between China and Austria pose as a proliferation risk.

This should be seen from the perspective that China is positioning itself as a rival to the West not only on an ideological level, but also in terms of security policy. Under President Xi Jinping, China has generally taken a more offensive stance and supports the proliferation efforts of nations that are hostile to the West.

Concrete threats to proliferation financing

Very common	frequently	regularly	rare
Financing the purchase of luxury goods for the DPRK regime	Financing the acquisition of dual-use goods	Financing the acquisition of proliferation-relevant goods	Raising funds to support a WMD programme.
Raising funds through foreign exchange for the DPRK regime	Sanctions are violated intentionally or negligently		Financing the acquisition of services or technologies
Concealment by legal entities (front			

companies, straw men)			

unless a country is specifically named, the DPRK and Iran are meant

Threat 1: Financing the purchase of luxury goods for the DPRK regime

The DPRK regime sends North Korean citizens abroad to fulfil state orders and act exclusively in the interests of the state. As a result, it is necessary to outline the status of these people within North Korean society. In order to secure long-term support and keep parts of the elite happy, it is essential to ensure regular material donations of luxury goods for the security apparatus. North Korean citizens sent abroad are instructed to procure high-quality products (textiles, leather goods, jewellery, precious metals, gemstones, watches, etc.) from the West on the basis of procurement lists, which are brought back to the DPRK via diplomatic mail or diplomatic baggage.

Threat 2: Raising funds through foreign exchange for the DPRK regime

DPRK pays for many of the necessities of its presence in Austria cash and in EURO. In principle, this is not reprehensible, especially as the financial sector cannot accept DPRK funds due to sanctions. However, the question of how the regime procures this cash remains unanswered. Activities such as the provision of a hostel in Berlin on embassy premises, whereby unsuspecting tourists hand over cash to the DPRK, are a knowen source of income.

Threat 3: Concealment by legal entities (front companies, straw men)

As citzens of North Korea or Iran can no longer enter into business relationships as natural persons in some sectors or listed persons cannot enter into business contact with Austrian companies, front companies and straw men are used to act as buyers, interested parties, etc. In addition, front companies and straw men act as a link between sellers and buyers of sanctioned goods without ever interacting operationally with the goods. To this end, front companies and front men act as a link between the seller and buyer of sanctioned goods without ever interacting operationally with the goods. Similar to money laundering or tax and duty fraud, these concealment structures can be complex in order to hide the beneficial owner. This also applies to trade financing, which is why a risk assessment by sector is possible (mechanical engineering, semiconductors, microelectronics and electronics).

Threat 4: Financing the purchase of dual-use goods

Dual-use goods are goods that can be used for both civilian and military purposes. This concerns components that can be used directly for the deployment or transfer of weapons of mass destruction, but also indirectly upstream goods that are used to produce goods for deployment and transfer. This usually concerns certain sectors, such as mechanical engineering, semiconductors, microelectronics and electronics (see also the goods under the export control lists). Dual-use goods are usually transferred to various destinations or stakeholders via bypass countries.

Threat 5: Sanctions are violated intentionally or negligently

If a natural person, organisation or company is newly included in the UN Security Council's sanctions list, there is a great deal of self-interest in withdrawing money or economic resources from Austria before a ban is imposed. There is a risk that sanctions could be violated by financial institutions.

Threat 6: Financing the acquisition of proliferation-sensitive goods

In addition to dual-use goods, proliferation-relevant goods are also acquired. As the detection threshold is higher due to increased awareness in the area of export control, customs of the relevant industrial companies, suppliers, credit and financial institutions and delivery companies, the probability of occurrence is generally lower. Proliferation-sensitive goods are all goods that are directly linked to the transfer, use and components of weapons of mass destruction.

Threat 7: Raising funds to support a WMD programme.

In principle, there is a risk that the DPRK and Iran will try to raise funds in Austria itself to support a WMD programme.

Threat 8: Financing the acquisition of services or technologies

Relevant services or technologies that are relevant to proliferation financing could also be procured in Austria. Abstract examples include technical-chemical companies based in Austria or high-security laboratories in Austria.

Which channels are used for proliferation financing?

Very high	high	medium	low
Cash	Front company	Cryptocurrencies	Bank transfers
		Hawala	

Method 1: Cash

Even if the DPRK regime is generally able to access bank accounts through nationals, for example, many goods and services are purchased by the regime itself using cash. Due to the lack of traceability of cash, an audit of the origin or use of funds is only possible in terms of customer due diligence.

Method 2: Front companies

In order to obtain proliferation-relevant goods, technologies or dual-use goods as described above, front companies or front men are used as intermediaries to conceal the actual beneficial ownership or the country of destination. This method is similar to money laundering or tax and duty fraud.

Method 3: Cryptocurrencies
As Austria is a dynamic location for Crypto Asset Service Providers (CASP), it can also be assumed that the DPRK and Iran are interested in using cryptocurrencies to conceal the origin or use of funds of assets or to attempt to gain access to assets via illegal access to Austrian CASPs.

Method 4: Hawala
Hawaladars in Austria engage in unauthorised business transactions by offering unlicensed payment services. Due to geographical and cultural proximity, it can be assumed that hawala can be used to support Iranian proliferation financing activities in particular.

Method 5: Bank transfers
Regular bank transfers via correspondent banking relationships, for trade financing or for front companies remain an interesting option, as large sums can still be moved in a short time, but more effort is required to conceal them due to extensive checks.

Risk minimisation measures

Proliferation and sanctions evasion or related illegal procurement processes pose a real threat to Austria. The DSN proactively contacts affected companies and research centres in order to draw attention to the dangers that can arise from proliferation and sanctions evasion through on-site awareness-raising measures. This preventative approach enables the DSN to prevent illegal procurement processes at an early stage. Technological developments are fast-moving, particularly in the field of dual-use technologies, which is why the responsible authorities are also committed to a regular dialogue with experts from industry and research.

The DSN also coordinates interministerial cooperation in national efforts to combat proliferation. Current national and international developments are discussed at regular inter-agency meetings and joint measures and their effects are debated.

In order to gain further insights into proliferation-related activities, the DSN commissioned a study in 2024. The Austrian corporate landscape was surveyed on this topic. Future approaches can be formulated on the basis of these findings.

Conclusion and risk classification

The fight against proliferation and its financing will continue to be one of Austria's central security tasks. The risk of weapons of mass destruction, delivery systems and the corresponding know-how coming into the possession of sanctioned regimes or terrorist organisations or of certain dual-use goods being misused for proliferation-relevant purposes contrary to official statements is one of the main proliferation-related threats. The proliferation of weapons of mass destruction

increases the potential international security risks and thus adversely affects the global security situation as a whole.

In this context, Austria is not only a transit country for proliferation-relevant goods, but also a destination country for illegal procurement activities due to its highly developed industrial production and the large number of small and medium-sized enterprises, which are global leaders in some areas. Dual-use goods, i.e. materials or products that can be used for both civilian and military purposes due to their technical specifications and high level of development, pose a particular problem.

Nevertheless, due to the fact that there are numerous companies in Austria that produce proliferation-relevant goods and the fact that state actors are willing to take covert measures to obtain these goods, the risk of proliferation-relevant activities and the linked necessary financing can be classified as **medium.**

6 Cross-sector risks in the property sector

The Austrian property industry is an important economic sector with strong national and international networks. Developments in this sector have a direct impact on the entire economy and the stability of the financial market. The property industry has a direct and indirect influence on the national gross domestic product. In 2023, the gross value added of the property industry amounted to around 42 billion euros, which corresponds to 9.76% of Austria's total economic output.

The international importance of the Austrian property industry is reflected in particular in its attractiveness for investors and the high transaction volume. In a study conducted in 2024, around 61% of investors surveyed rated Austria as an attractive location for property investments. This high popularity is reflected in investment activity, as the transaction volume of property investments in Austria was €4.55 billion in 2021, an increase on the previous year. Due to Austria's economic stability and attractiveness for investors, the property sector plays a central role in capital flows.

In Austria, however, the acquisition of property rights by third-country nationals is restricted by provincial legislation. Authorisation from the Land Transfer Commission or a negative confirmation is required if the acquirer of rights is not a citizen of the European Union exercising the fundamental freedoms under EU law (in particular the free movement of capital pursuant to Art. 63 TFEU, which includes real estate as tangible capital in the scope of protection) or a person treated as a national on the basis of the EEA Agreement. This authorisation requirement applies equally to foreign natural persons and legal entities. The national legal bases for foreign property transactions are as follows:

- Burgenland: § 2 para 7, § 4, § 11 Bgld GVG 2007
- Carinthia: § 6, § 13, § 15 K-GVG 2002
- Lower Austria: § 3 para 6, § 4, § 6 NÖ GVG 2007
- Upper Austria: § 2 para 4, § 8 Oö. GVG 1994
- Salzburg: § 21, §§ 24 ff. S.GVG 2023
- Styria: § 22 para. 1, § 25, §§ 27 f. (Styria) GVG 1993
- Tyrol: § 2 para 7, §§ 12 f. (T)GVG 1996
- Vorarlberg: § 2 para 7, §§ 7 f. Vlbg GVG 2004
- Vienna: § 2, §§ 4 f. WrAuslGEG

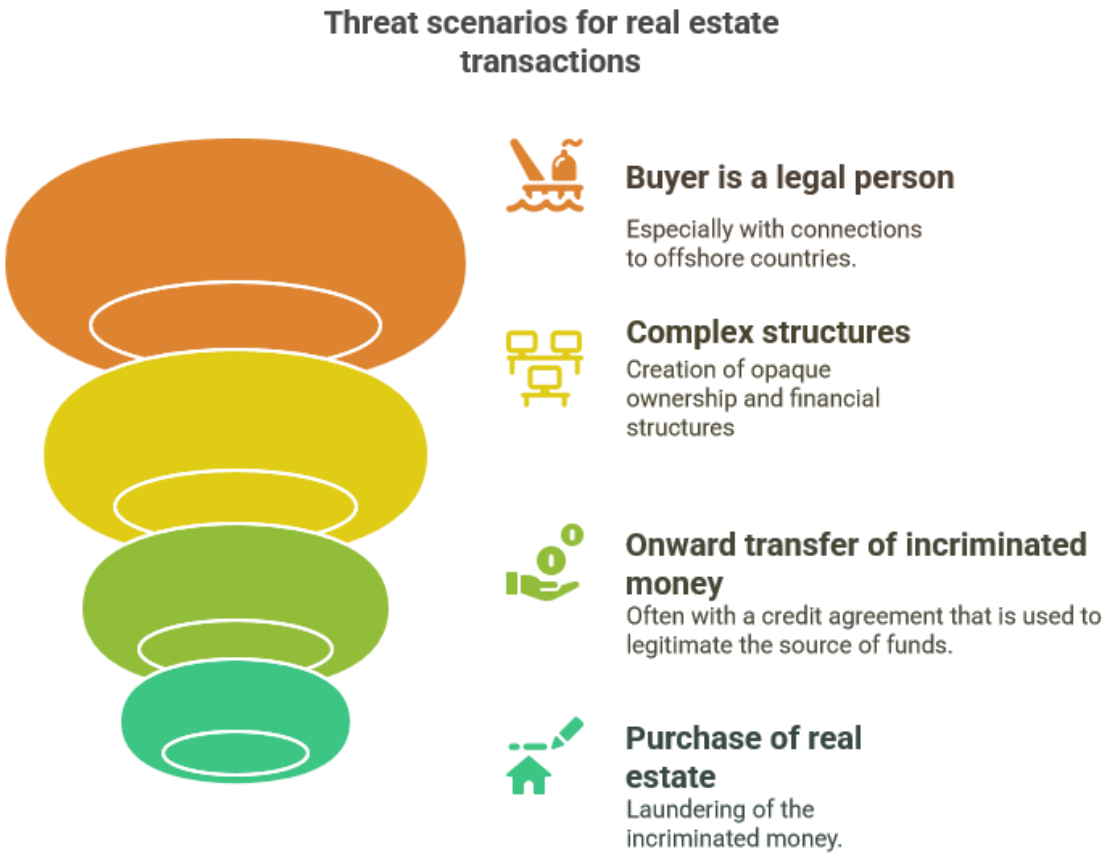
In some cases, these provincial legal provisions represent significant barriers to the acquisition of land by third-country nationals.

This analysis presents cross-sector risks in the property sector. The risk classification is carried out as part of the respective sectoral risk assessments of the occupational groups.

Money laundering risks in the property sector

The property sector offers an attractive opportunity for illicit financial flows due to the high value stability of real estate and the possibility of moving large sums of capital. As Austria is a popular location for national and international investors, certain patterns and risks can be observed that indicate the use of real estate for the purposes of alleged money laundering. In practice, there are a variety of methods for laundering money through property transactions.

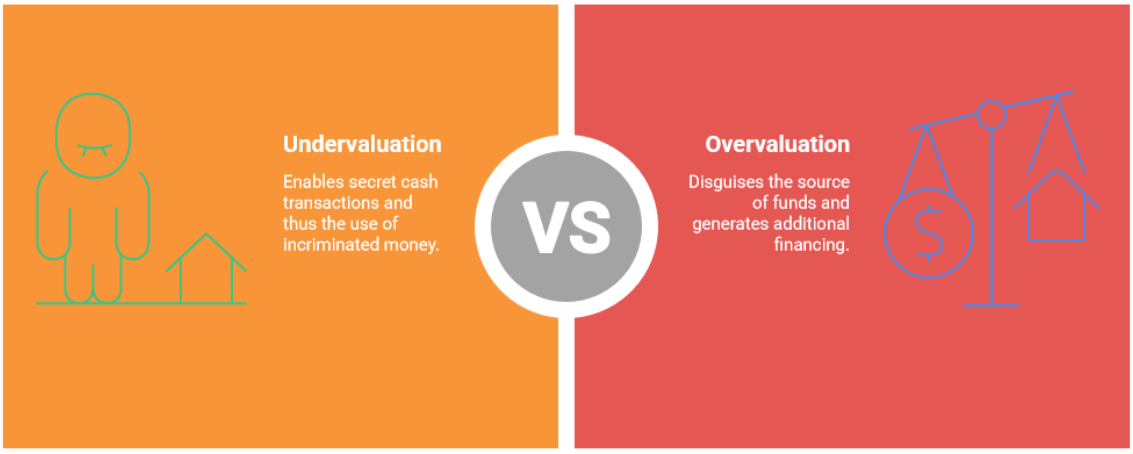
In practice, one risk scenario that can be observed is that domestic or foreign legal entities are used for the purchasing party when buying a property or real estate. These are often entangled in a network of companies with links to offshore destinations in order to create complex financial structures and opaque organisational structures. Incriminated money is channelled through this network and often passed on to the purchasing company by means of a loan agreement. In this way, the illegally generated funds are channelled into the company and, when asked, the loan agreement is cited as proof of the origin of the funds. In such cases, countries with weaker financial control mechanisms are chosen for the company headquarters in order to avoid monitoring and benefit from an inefficient enforcement mechanism.



Furthermore, the purchase of existing shelf companies also plays a role in Austria time and again. Shelf companies are pre-established companies (mainly limited liability companies) that have not yet developed any business activities or existing companies that no longer carry out any business activities. The advantage for criminals is that they are already entered in the company register and have a bank account with paid-up share capital as well as a tax number. The purchase of such companies saves time and effort compared to setting up a new company, but offers a high potential for abuse. Such companies can be used quickly to process transactions and can also be quickly replaced by other shelf companies if the unlawful activities are discovered. These characteristics represent potential vulnerabilities. It is also becoming increasingly apparent that these steps are being taken by utilising the legal advisory professions and the various services they provide.

Another method that has been observed by the authorities is the undervaluation or overvaluation of properties. The aim of undervaluation and overvaluation is to conceal the actual value of the property and to inconspicuously introduce illicit money into the purchase process. In the case of undervaluation, properties are knowingly sold at a price below their market value. However, the difference to the actual value is paid in cash under the table. This method offers money launderers an opportunity to invest black money and thus launder incriminated funds. In contrast, overvaluation involves deliberately overstating the value of a property in order to disguise the origin of the funds or generate additional financing.

How are undervaluation and overvaluation of property used for money laundering?



Internationally, it is also evident that nested ownership structures and opaque transactions are increasingly being used to conceal money laundering and other illegal activities. Nationally, this poses a challenge for regulatory authorities, as the property market not only has economic implications, but also security implications. The threat of money laundering in the property sector in Austria is therefore classified as medium to high.

Terrorist financing risks in the property sector

In Austria, legal sources of financing and the use of funds for terrorist organisations and individuals are used, such as fundraising, earned income and social assistance. Fundraising through criminal offences (robbery, theft, fraud, etc.) has not been identified to date. In general, it should be noted that income can be generated through the trading and letting of property, which can then be misused for terrorist purposes. The property sector is therefore not protected against terrorism financing. However, there are currently no recognisable indications of terrorism financing in the Austrian real estate sector. Even though the risk potential in the property sector is classified as low, the sector remains under close observation by the competent authorities due to its economic importance and the potential risks of abuse.

Proliferation financing risks in the property sector

The term proliferation refers to the spread of nuclear, biological and chemical weapons of mass destruction, the delivery systems required for them and the products used to manufacture them, including the necessary expertise. Proliferation financing refers to the provision of financial resources or services to support the proliferation of these weapons of mass destruction. The sanctions applicable in this context are directed against the financing of the North Korean weapons of mass destruction programme. Due to the far-reaching control exercised by the North Korean government, all economic activities of North Koreans are subject to sanctions.

In recent years, it has been revealed several times that North Korean diplomats and embassies not only use real estate for official purposes, but also use it specifically to finance proliferation. The procedure follows a recurring principle. A North Korean diplomat buys a property abroad, which is then rented out to a third party. The rental income is not reinvested in the respective host country, but transferred directly to North Korea. A similar variant is the commercial utilisation of diplomatic properties or real estate. Accommodation or a business is set up within the embassy or an official building and services are offered for a fee. The profits generated from this in turn flow to the North Korean government. A striking example of this pattern is the conversion of diplomatic facilities into short-term rental properties. In the past, for example, embassy premises were run as hostels and guests were accommodated for a fee. These cases have shown that diplomatic structures are deliberately used to generate foreign currency, with the revenue then presumably flowing into prohibited programmes, in particular the development of nuclear weapons. Since 2017, UN Resolution 2321 (2016) has prohibited North Korea from using real estate on the territory of other countries for non-diplomatic purposes. The international cases show that strict monitoring and control of proliferation financing by the authorities is essential.

Obliged entities affected

Various obliged entities are directly affected by the risks of money laundering, terrorism financing and proliferation financing in the property sector and therefore bear a significant responsibility in preventing these risks. A property acquisition usually has points of contact with various obliged

entities. On the one hand, lawyers, notaries and estate agents are involved and, on the other, banks that handle the property transaction. Therefore, there are many ways to prevent incriminated activities before the transaction is finalised through sufficient prevention.

1. Financial and institutions

Compared to other methods, the property sector offers a comparatively simple way of transferring illegal assets into the legal economic cycle. Criminal funds can be smuggled in during the initial phase through the acquisition of property and then concealed through various transactions. Once the integration is complete, the properties can either be sold on at a profit or utilised in the long term. Credit and financial institutions are among the central players affected by the risks in the Austrian property sector in connection with money laundering, terrorism financing and proliferation financing. Due to their role in the financing and processing of transactions, they have a special responsibility to recognise and prevent illegal money flows at an early stage. The Austrian property market is attractive for criminal actors due to the high investment sums and long-term stability of value, who channel illegal funds into the legal economic cycle through nested ownership structures, offshore companies or overvalued property purchases. Credit and financial institutions must therefore apply increased customer due diligence in order to closely examine the economic background of transactions and minimise the risk of money laundering. Trust accounts, which are managed by agents or brokers and can make it difficult to trace the origin of funds due to the large number of transactions involved in a transaction, are an instrument for concealing the origin of illegally acquired funds. Attractiveness in connection with money laundering also results from the fact that it is a largely stable investment that can be acquired with cash and whose value can be increased through revaluation measures.

Anomalies can include multiple purchases or resales of properties with conspicuous price deviations from the actual value, financing via offshore lenders, the use of intermediaries to disguise the involvement of individuals, or the acquisition of a property with no recognisable connection between the buyer and the country.

In addition to money laundering, there is also a potential risk in the area of terrorism and proliferation financing. Real estate can be used specifically as a store of value or as an instrument for circumventing international sanctions. Investments by sanctioned actors or straw men who conceal their true identity through complex corporate structures are particularly critical. Credit and financial institutions are therefore obliged to carefully check business partners and customers in order to rule out links to sanctioned states or organisations. Regular sanctions list checks, increased identification of beneficial owners and a detailed analysis of suspicious transactions are therefore essential in order to reduce financial and legal risks for a financial institution and fulfil regulatory requirements.

2. Notaries

In all business areas susceptible to money laundering**, the threat of abuse for money laundering** lies in the fact that the involvement or processing of the transaction via notaries could suggest harmlessness and respectability. If bank accounts are involved, there could also be a risk that banks

will scrutinise notaries less strictly as account holders. A classic threat scenario could be the attempt by perpetrators to conceal the origin of illegally obtained assets when buying/selling property or companies in the area of money laundering by investing in the property sector or buying large amounts of companies. The illegal origin of high proceeds from criminal activities could be concealed "in one fell swoop" and thus "laundered clean". Such investments could also allow the creditworthiness of acquired companies to be used for further criminal activities (e.g. by taking out loans). In the area of money laundering, classic threat scenarios could involve perpetrators attempting to set up companies with the help of notaries in which "straw men" are used as shareholders and/or managing directors to conceal the origin of assets or beneficial ownership, or in which shell companies are transferred for the same purpose. In addition, the purpose of managing money, securities or assets, opening or managing bank, savings or securities accounts and establishing and managing companies or foundations may be to conceal illicit funds through financial transactions or the establishment of entities. [1]Another threat scenario could also be posed by bogus companies that seek to conceal the illegitimate origin of assets through strategic property investments or large-scale company acquisitions, or that are set up for the purposes of social and tax fraud. In this case, there could be a risk of attempts to use notaries to set up companies or transfer shares.[2]

In all money laundering-related business areas, the **threat of abuse for terrorism financing** lies in the fact that the involvement or processing of the transaction via notaries could suggest harmlessness, respectability and creditworthiness. If bank accounts are involved, there could also be a risk that banks will scrutinise notaries less strictly as account holders. When buying/selling property or companies, a classic threat scenario could be an attempt by perpetrators to obtain assets for terrorism financing purposes by investing in the property sector (e.g. through profitable investments). However, classic threat scenarios in the area of terrorism financing could also include attempts to use notaries as "front men" for asset management, the opening of donation accounts as a cover for collecting money and the establishment and management of companies in order to generate funds for terrorism financing.

In all business areas **at risk of proliferation financing, the threat of abuse is** that the involvement or processing of the transaction via notaries could give the impression of harmlessness and respectability. If bank accounts are involved, there is also a risk that banks will not scrutinise notaries as account holders as strictly, which could facilitate misuse to finance the proliferation of weapons of mass destruction. Classic threat scenarios for notaries in the context of proliferation financing include attempts to use them to process transactions that serve to finance the proliferation of weapons of mass destruction. This could be done by setting up and managing companies or foundations that are used as a cover for the transfer of funds, particularly in relation to high-risk countries such as the Islamic Republic of Iran or the Democratic People's Republic of Korea (DPRK). The opening and management of bank accounts via notaries can also be misused to disguise the origin and intended use of the funds, thereby concealing the actual intention.

[1] Further information can be found in the notaries' sectoral risk assessment
[2] Further information can be found in the notaries' sectoral risk assessment

Special care must be taken when handling property and company transfers if unusual payment structures or complex company law constructions are involved. Careful examination of the beneficial owners and payment flows helps to gain a comprehensive understanding of the background to a transaction and minimise the risks of money laundering, terrorism financing and proliferation financing.

3. Lawyers

In all transactions that are subject to customer due diligence**, the threat of abuse for money laundering** lies in the fact that the involvement of a lawyer or the processing of the transaction via a lawyer could create the appearance of harmlessness, legitimacy and respectability. Lawyers have a special position of trust in society and criminals can try to abuse lawyers by using them as a "seal of approval" for certain transactions.

Criminals may attempt to create complex and opaque structures involving multiple jurisdictions, particularly offshore jurisdictions with disguised ownership. This often involves the owner of another company or legal structure being registered in another jurisdiction. This combination of different legal services in different jurisdictions may be an attempt to deliberately add complexity to the transaction.

The acquisition of real estate or companies and company shares by persons domiciled or resident outside the EU/EEA and the establishment of new companies for use in criminal activities pose an increased potential threat in terms of money laundering. In such constellations, acquisition companies are often set up specifically for the purchase and are backed by numerous complex, nested legal entities. This can make it considerably more difficult to identify the beneficial owners and the origin of the funds in Austria. Similar risks also exist when setting up (acquisition) companies for the purpose of managing assets (such as shareholdings).

In contrast, the threat scenario in connection with the opening and management of bank, savings and securities accounts or trusts, foundations and similar structures by lawyers is considered to be lower. Lawyers working in Austria are particularly sensitive to the issues of money laundering, terrorism financing and proliferation.

The assessment of vulnerability to **terrorism financing** in connection with legal services provided by lawyers is generally considered in conjunction with money laundering schemes designed to conceal the illegal origin of the funds. Threat scenarios include, for example, the raising of funds through donations to non-profit organisations for which lawyers can act as advisors in the establishment of such organisations. Possible, but not yet observed in practice, is the opening of accounts by lawyers, the use of lawyers as straw men in asset management or money transfers by lawyers via other accounts.

There is a possibility that the purchase or sale of real estate could be misused for terrorism financing. However, there would have to be additional elements, such as forwarding the proceeds of the sale

to dubious organisations, countries or individuals. As a rule, however, the lawyer is not involved in this.

The involvement of a lawyer in the purchase and sale of companies for terrorism financing purposes is also rather atypical, as terrorism financing usually requires liquid funds quickly and sustainable investments in companies are therefore not suitable for terrorism financing purposes. In the case of corporate transactions, further circumstances would therefore have to be added, in particular with regard to the forwarding of sales proceeds to the corresponding recipients, in which lawyers are not involved or which are no longer part of the (typical) corporate transaction.

Threats exist due to Austria's historically close business contacts with Iran. In the past, arms deliveries were also made to Iran, which led to the tightening of the relevant control regulations and can no longer be carried out today. Austria also has a strong financial system with international connections that could be vulnerable to **proliferation financing.** Structures involving third countries that serve to circumvent sanctions are conceivable.

With regard to North Korea, the main theoretical risks are the circumvention of sanctions by third parties and trade in illegal goods to finance proliferation. There are also reports of sports clubs that have contacts with the North Korean regime.

4. Estate agents

Property transactions offer criminals the opportunity to channel illegal funds into the legal economy. The high sums involved and the stable value of property make it attractive for **money laundering activities**. Estate agents could become involved in such schemes, especially if they do not apply appropriate customer due diligence. For example, complex ownership structures or the use of straw men can be used to disguise the true origin of funds.

In addition to the risk of money laundering, estate agents must also protect themselves against misuse to **finance terrorism**. There is a risk for estate agents as, in principle, all properties are suitable for investing funds that can later be used for terrorist purposes or possibly serve directly as a starting point for terrorist activities.

Estate agents are exposed to the risk of **proliferation financing**, as real estate can be used as a stable value investment to conceal illegal funds from high-risk countries. Particularly problematic are complex ownership structures, offshore companies and trusts that disguise the true origin of the funds and thus enable the circumvention of international sanctions. Brokers can unwittingly facilitate transactions that serve to finance weapons of mass destruction, especially if they do not carry out careful identity checks.

5. Indicators for obliged entities:

There are numerous indicators that suggest that obliged entities could be misused for the purposes of money laundering, terrorism financing or proliferation financing. The following list of possible indicators for detecting anomalies in relation to money laundering, terrorism financing and proliferation financing is exemplary and is intended to provide obliged entities with possible indications of suspicious circumstances.

- Insistence on cash payment or unusual cash transactions
- Creating time pressure to close the deal
- Refusal to provide customary information without giving reasons
- Discrepancy between acting persons and business, e.g. if the intended business does not suit the customer in terms of age, knowledge, etc.
- False or misleading information provided by the customer
- Customers who conspicuously avoid direct contact or overly conspicuously seek contact with certain employees
- Transactions that do not appear plausible due to geographical distance from the customer's place of residence
- Complex legal structures whose ownership or control relationships are difficult to clarify and understand
- Transactions with countries that offer corporate structures that make it difficult to identify and verify the origin of funds and where, according to credible sources, there is an increased risk of money laundering and terrorism financing.
- Recent change of all shareholders and management, or change of registered office as an indication of the use of a shelf company
- Missing or incomplete information in the payment order
- Payment with virtual currencies (especially if not agreed in advance and not in line with the business model)
- Foreign travel paid by the customer for business transactions
- Unusual or conspicuous business practices in connection with high amounts
- Repeated changes to the agreed arrangements
- Life insurance policies: Implausible transactions (premium amount and motives), irregular payments, cash payments, conspicuous or unreasonable surrenders of life insurance policies
- Concealment of fiduciary relationships or beneficial ownership, e.g. through offshore structures
- Payment or delivery by unknown or uninvolved third parties
- Repeated postponements/excuses when providing documents

7 Cross-sector risks of means of payment and payment and financial transfer systems

The world of payment methods is undergoing dynamic change, which is largely shaped by technological advances, globalisation and changing consumer preferences. In Austria, cash continues to play a central role in payment transactions. Cryptocurrencies and unlicensed payment service providers, such as unlicensed crowdfunders and unofficial financial transfer systems such as Hawala or Fei Chien, will also be examined. Due to their anonymity, their lack of regulation in Austria and many other countries and their difficult verifiability, these means of payment harbour considerable risks of money laundering, terrorism financing and proliferation financing.

A differentiated picture can be seen internationally. In many countries, particularly in Scandinavia and parts of Asia, digital and mobile payment methods are becoming increasingly important and have in some cases replaced cash as the dominant means of payment. These developments reflect the global trend that is leading to more cashless payment transactions in many regions. The increasing use of these technologies enables greater flexibility and efficiency in payment transactions, but also creates new challenges in areas such as money laundering, terrorism financing and proliferation financing. These risks require an adapted regulatory framework and continuous monitoring to ensure the integrity of the financial system worldwide.

This analysis presents cross-sector risks in the property sector. The risk classification is carried out as part of the respective sectoral risk assessments of the occupational groups.

1. Cash

Despite the increasing trend towards cashless payment methods, cash is still very popular, especially in Austria. According to the European Central Bank's (ECB) SPACE 2024 payment method survey, 62% of transactions at the point of sale (POS) in Austria were carried out with cash, which is around 10 percentage points above the eurozone average.[3] 38% of Austrian consumers still prefer cash, almost twice as many as the eurozone average (22%). However, in 2024, card payments (39%) will be more popular than cash for the first time in Austria, which was still the preferred payment method for almost half (45%) of Austrians in 2022.

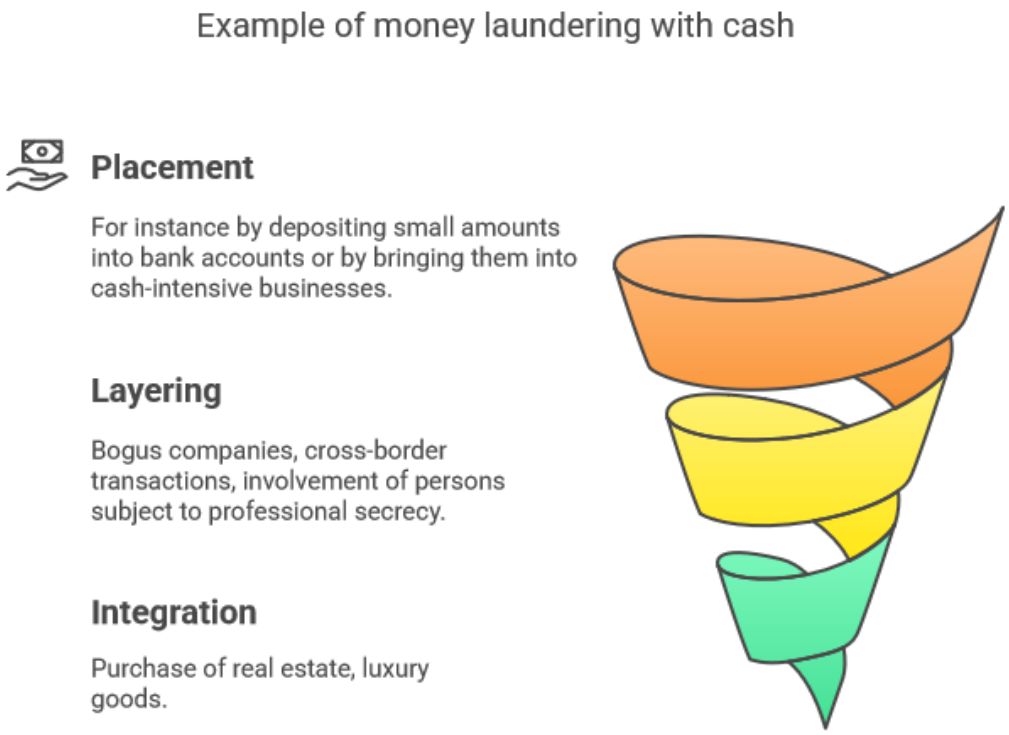
[3] See OeNB of 19 December 2024, Cash remains the most widely used means of payment at the point of sale in the eurozone at 52% - Oesterreichische Nationalbank (OeNB)

There is currently no statutory cash limit in Austria.[4] Instead, there is an identification requirement for cash payments of EUR 10,000 or more for transactions with obliged entities. In accordance with the applicable money laundering regulations, there is an obligation to apply customer due diligence when carrying out certain cash transactions. This applies, for example, to traders who accept cash payments of at least EUR 10,000 or cash transfers of more than EUR 1,000. In the construction sector, there is also a ban on cash payments for wage payments for construction services and a ban on deducting operating expenses for cash payments between entrepreneurs.

Money laundering

The three-phase model is often used to describe the complex process of money laundering. This is divided into the phases of placement, concealment and integration. In the placement phase, the illegally acquired (cash) money is first channelled into the economic cycle, for example by depositing small amounts into bank accounts or by placing it in cash-intensive businesses such as casinos. In the subsequent concealment phase, the actual origin of the money is disguised. For this purpose, complex cross-border financial transactions are often carried out, offshore and letterbox companies are set up or professional secrecy holders such as lawyers or notaries are involved, whereby cash in excess of €1,000 must be deposited in escrow accounts with notaries and no cash transactions take place. In the final integration phase, the apparently legal funds are returned to the regular economic cycle, for example through investments in companies, the acquisition of real estate or through allegedly legally generated income from gambling services or other sham transactions.

[4] From 10 July 2027, a uniform cash payment limit will come into effect throughout the EU, including in Austria. The Regulation limits cash payments to a maximum of €10,000 and covers both transactions between companies and transactions between companies and consumers.



The processes described illustrate that cash can be a favoured means of money laundering due to its anonymity.

A popular method of money laundering is the use of bogus companies. Such companies are used to conceal the traces of money movements. Illegal funds are declared as alleged income from these bogus companies. After being recognised as profit or income, the money can then be used as apparently legal funds. So-called sham invoices are also frequently used in this context. A bogus company creates fictitious invoices that are formally correct but are based on services or deliveries that were never provided. The money is then "laundered" by paying these invoices.

Bogus companies often serve as one of the intermediaries for forwarding the money. This can be done through transfers to other companies, offshore accounts or investments in property or crypto assets. They are also often set up in tax havens or countries with weak financial supervision. The true owners remain anonymous and there is no obligation to make annual reports or tax returns publicly available.

Particularly in the final phase of money laundering, the reintegration of the laundered assets into the regular economic cycle, the originally illegal but now seemingly legal assets are suitable for the purchase of luxury goods, such as jewellery or high-priced designer goods. Traders can be misused for money laundering purposes. Such luxury items are particularly attractive to criminals because of their stable value. Particularly in the area of high-value luxury goods (such as watches or handbags),

considerable increases in value can even be achieved when resold. However, traders can be involved at earlier stages of the money laundering process, often involuntarily. If the legal customer due diligence requirements are not implemented properly, acts of concealment could be facilitated, for example by the purchase of assets of illegal origin. The consistent application of money laundering prevention regulations could prevent such transactions in advance. Increased control measures by the competent supervisory authorities can also make a significant preventive contribution to the fight against money laundering. Inadequate application of customer due diligence can enable concealment, for example through the purchase of incriminated jewellery. The application of anti-money laundering regulations and official controls can counteract such risks preventively.

Terrorism financing

Cash plays a central role in financing terrorist activities as it is anonymous, difficult to trace and easy to transport. Unlike digital payment systems, cash leaves no direct trace of transactions, making it particularly attractive to criminal networks. Terrorist groups use cash for various purposes, including procuring weapons, organising attacks and maintaining their infrastructure.

Within the Austrian financial sector, risks in connection with terrorism financing can result from the monitoring of cross-border transactions, the screening of customers from high-risk regions and the control of certain cash-intensive business areas. According to Annex III of the Financial Markets Anti-Money Laundering Act (FM-GwG), cash-intensive companies are explicitly categorised as factors that potentially represent an increased risk in accordance with article 9 (1) FM-GwG.

Credit and financial institutions with large remittance flows or a broad customer base may be exposed to increased risk if their systems are unable to recognise smaller, fragmented transactions that are potentially linked to terrorist activities. In addition, deficiencies in the implementation of legal requirements, such as the irregular updating of sanctions lists or the existence of incomplete KYC information, increase these risks.

2. Virtual currencies (crypto assets) and cryptoassets

In recent years, virtual currencies (crypto currencies) and crypto assets have become increasingly important and represent an innovative alternative to traditional means of payment and investments. While virtual currencies (crypto assets) are digital means of payment that are mostly used in closed systems or online platforms, crypto assets go beyond this and include a wide range of digital assets based on blockchain technology. Bitcoin and Ethereum are particularly well known, but stablecoins, security tokens and other digital assets are also gaining in relevance. In this context, providers of crypto asset services such as crypto exchanges, wallet providers and other financial intermediaries that trade in these digital assets have become increasingly important.

Money laundering

The methods for money laundering are widespread in the crypto-asset sector due to the existing pseudonymity and rapid processing. The risk of money laundering is also increased by virtual assets, which enable individuals and organisations to transfer funds across borders with minimal supervision. Furthermore, the general challenges of crypto-assets remain the complex tracking of cash flows, the use of mixing services or the disbursement of funds by rogue exchangers based in uncooperative or weakly regulated countries. The attractiveness of crypto-assets for fraud and money laundering remains unchanged. Criminals take advantage of the highly complex technology and the victims' lack of expertise, coupled with the possibility of quickly removing the funds from the authorities' grasp. In Austria, it has been repeatedly noted that the use of stablecoins in particular is often used for fraudulent activities. Stablecoins are virtual currencies whose value is linked to an anchor value, such as a fiat currency, often the euro or US dollar. The aim of stablecoins is to avoid the typical high volatility while retaining the advantages of crypto assets. Due to their stability, stablecoins are particularly popular with fraudsters because the incriminated assets are only subject to a low price risk.

In the crypto sector, the "peel chain" method of money laundering is relevant, in which large sums of illegal money are divided into numerous small transactions ("peeled off") and fed back into the regular financial cycle via various, often lightly regulated or decentralised crypto exchanges. Decentralised platforms (DeFi), which are based on smart contracts and often use stablecoins such as Tether (USDT), offer additional anonymity due to the lack of intermediaries.

Money mules are now regularly used by (financial) fraudsters in connection with crypto exchanges. Money mules are people who are lured with job offers. They are then instructed to open accounts with known crypto exchanges and to receive funds in their bank account on behalf of the company and to convert and transfer them to their crypto accounts.

Terrorism financing

The use of virtual assets by terrorist organisations harbours considerable risks. They can enable fast and pseudonymous cross-border transactions, making it difficult to trace the origin and destination of funds. Terrorist groups can exploit this lack of transparency to fund their activities. According to

the SNRA, crypto-asset service providers pose a significant risk for terrorism financing due to gaps in regulation and supervision.
Anonymity-enhancing crypto-assets (AECs) in particular can be used in terrorism financing. For example, ISIL, Al-Qaeda and their affiliated groups have utilised crypto-assets such as Monero to raise and distribute funds in Africa, Europe and the Middle East. In addition, virtual assets, often in conjunction with crowdfunding platforms, have also been increasingly used to finance right-wing extremist terrorist activities.

3. Non-licensed payment service providers

Non-licensed crowdfunding providers

Crowdfunding is an alternative form of financing in which capital is provided by a large number of people via specialised online platforms. Supporters invest in a project, a company or a business idea without the need for traditional sources of financing such as banks. Due to the high level of anonymity and easy accessibility on public websites, there are risks of money laundering, terrorism financing and proliferation financing. This risk has already been partially addressed by the legislator by making at least the most common types of *crowdinvesting* platforms subject to AML obligations: On the one hand, providers under the Crowdfunding Regulation (Regulation (EU) 2020/1503), and on the other, national providers based on the Alternative Financing Act (AltFG). In principle, crowdfunding platforms are also generally not permitted to transfer payments between their customers, but must use regulated payment institutions to do so.

Money laundering

Crowdfunding can be an attractive target for money laundering, as a large number of small transactions can disguise the origin of illegal funds. There is a risk that criminals may invest illegally acquired funds in seemingly legitimate projects, particularly in the case of less regulated platforms or anonymous donations. However, the current information and data situation does not provide any concrete indications of a threat in Austria that crowdfunding is being misused for money laundering purposes.

Terrorism financing

In Austria, the unregulated "donation-based" crowdfunding sector in particular could be misused for terrorism financing purposes with relatively simple means. Terrorists or their supporters can use these crowdfunding opportunities to raise funds for terrorist purposes or to support terrorist activities. Terrorist organisations mainly receive funds from sympathisers and are very clandestine in their approach. The more the donors can identify with the organisation's "cause", the easier it is to raise funds. Sympathisers of terrorist organisations often only have very limited financial resources. Nevertheless, it is known that considerable sums can sometimes be raised through fundraising. The money is collected via projects on unregulated crowdfunding platforms, but increasing international attention is also being paid to fundraising by non-profit organisations, the

proceeds of which can be used for terrorism financing. The true purpose is (usually) unknown to many small donors. In addition, giving a donation is a commandment in many religions and usually consists of small and very small amounts. In well-organised groups, (cultural) associations are run to cover the true purpose, whereby the cultural purpose of the association is placed in the foreground to the outside world. Based on the available information and data, such threat situations may also arise in Austria.

Informal financial transfer systems

Well-known systems of this type are Hawala, Hundi, Fei Chien, Phei Kwan and Padala, which, despite regional differences, use similar mechanisms to transfer money efficiently and often cost-effectively across national borders. These systems became known to the wider public in particular in connection with the terrorist attacks in the USA in 2001, when investigators established that Hawala was used as the main financial transfer system for carrying out these attacks.

A typical transaction via an informal financial transfer system takes place between a money sender, two corresponding intermediaries (so-called middlemen) and a money recipient. The system is based on a network of intermediaries who operate on the basis of mutual trust. A person wishing to transfer money to another country hands over the amount to a local intermediary, also known as a hawaladar. The intermediary forwards instructions to a partner in the destination country. The recipient then receives the amount from this partner, using a previously agreed password. In most cases, such transactions can only be traced through the strictly kept books of the respective intermediary.

Money laundering

The use of informal financial transfer systems for money laundering of incriminated funds remains a high risk. Often, such a structure can only be uncovered by chance during other investigative activities, as various commercial enterprises (e.g. jewellers, mobile phone shops, restaurants) are used as a cover to carry out money transfers in the background. In connection with such financial transfer systems, evidence has repeatedly been found that they are used to finance illegal activities. In particular, there have been links to human trafficking, drug trafficking and terrorism financing. Tracing is made more difficult by the use of such a system, as the identity of the sender or recipient is difficult to establish and regulated countermeasures are deliberately circumvented. The attractiveness of these systems lies in the minimal documentation and the lack of traceability, as several intermediaries and countries can be involved in the process and the funds pass through several intermediaries before reaching the final recipient. Newer forms of so-called "Chinese Underground Banking" use, among other things, bogus companies to carry out transactions and thus transfer funds incriminated in Europe to distant countries.

Terrorism financing

Terrorism financing funds are almost exclusively transferred to third countries (e.g. the Russian Federation, Turkey, Middle Eastern countries, Somalia, Afghanistan, Pakistan, Iraq or Syria). Due to the frequent transfer via several third countries, it can be difficult to reliably identify the final recipient country and the actual recipient. In addition, there is evidence of money transfers from relatives of people close to them who have travelled to crisis regions to join the armed jihad, have already joined it or are currently travelling there.

On the one hand, funds are transferred via official financial service providers (Money Value Transfer Services, MVTS). However, if this is not possible or expedient, for example due to a lack of bank details in the destination country, the funds are transferred via unofficial intermediaries. Any number of intermediaries can be used to disguise the final destination. Terrorist organisations use cash couriers when large sums need to be transferred in order to avoid the strict requirements regarding the prevention of money laundering and terrorism financing.

Apart from legal financial service providers such as banks and financial transfer service providers, trustworthy contact persons in the country of origin or destination are entrusted with the transaction, even though this is generally not legally permissible due to the trusteeship assumed. These trusted contacts are usually co-nationals or at least people from the same cultural background.

8 Sectoral risk assessment of legal entities and trusts

8.1 Domestic legal entities

General description

General information on sector / product / service / activity:
Legal entities and trusts can be misused for the purposes of financing terrorism or proliferation or for money laundering. Based on the guidelines of the FATF, the Supranational Risk Assessment of the European Union and, the methodology of the European Global Facility, a methodology tailored to Austria has been developed. The risk assessment is carried out at the level of each legal form that can be established in Austria. A separate analysis was carried out for foreign legal entities that have a suficient link to Austria. In order to assess the risk, the following three basic scenarios can be evaluated:

- Formation of legal entities, trusts and trust-like agreements with the aim of concealing the beneficial ownership thereof (relevance: 45%);
- Business activities of legal entities, trusts and trust-like agreements that may serve the purpose of financing terrorism or proliferation or money laundering (relevance: 45%);
- The liquidation of insolvent legal entities, trusts and trust-like agreements with the aim of purchasing the assets from the former owner and continuing the same business activities (relevance: 10 %).

The schemes and red flags for the baseline scenarios were included in the threat and vulnerability assessment (part of the inherent risk assessment), which is why no separate results were assessed for these scenarios.
This analysis also forms the basis for the risk-based supervision of the beneficial ownership register.

General information on the usual legal forms:
In a first step, the following legal entities were categorised as relevant:

Legal form	Number of legal entities	Description of the legal form	Main register and competent authority	Website

Stock corporation	891	In accordance with the Stock Corporation Act (AktG), a stock corporation (AG) is a legal entity that is itself the holder of rights and obligations. It is a corporation with a minimum share capital of 70,000 euros, which is divided into shares. A stock corporation whose shares are not listed on a stock exchange or traded via a multilateral trading facility (MTF) may only issue registered shares in accordance with article 9 AktG and must keep a share register (article 61 AktG). Listed stock corporations and companies whose shares are traded via a multilateral trading facility (MTF) may also issue bearer shares in accordance with article 10 AktG. However, all bearer shares must be securitised in a global certificate and deposited with a central securities depository.	Company register Regional courts and the Commercial Court of Vienna	https://justizonline.gv.at/jop/web/firmenbuchabfrage
Limited liability company	201.625	According to the Limited Liability Companies Act (GmbHG), a limited liability company (Llc) is a legal entity that is itself the holder of rights and obligations. It is a corporation with a minimum share capital of EUR 10,000, at least half of which (EUR 5,000) must generally be paid in cash when the company is founded. The	Company register Regional courts and the Commercial Court of Vienna	https://justizonline.gv.at/jop/web/firmenbuchabfrage

		shareholding structure can be found in the Austrian commercial register.		
Flexible company	762	The new Austrian flexible company, which was introduced on 1 January 2024, is comparable to a limited liability company, but has some special features. For example, less than 25% of the share capital may be "enterprise value shares". These Enterprise Value Shares have no voting rights and must be kept by the company in a share register. The specific amount of the individual Enterprise Value Shares cannot be retrieved from the company register. In addition, the company itself can acquire both business value shares and enterprise value shares, which also have no voting rights. When reporting, particular attention must be paid to the distinction between ownership and voting rights. As enterprise value shares and treasury shares do not have voting rights, the voting rights of the other shareholders increase accordingly. Thus, the amount of shares and the amount of voting rights will regularly diverge and beneficial ownership will be determined by the amount of voting rights. It should also be noted that beneficial ownership can also	Company register Regional courts and the Commercial Court of Vienna	https://justizonline.gv.at/jop/web/firmenbuchabfrage

		result from the aggregation of shares and enterprise value shares.		
General Partnership	22.139	General partnerships and limited partnerships are partnerships established in accordance with articles 105 ff of the Austrian Commercial Code (UGB), which are entered in the publicly accessible company register and have legal capacity. They can therefore have rights and obligations, enter into liabilities and also sue and be sued. A registered partnership consists of at least two partners who, in the case of a General partnership, have unlimited and joint and several personal liability. In the case of a limited prtnership, at least one partner has unlimited liability (general partner), while the liability of at least one other partner is limited to their liability amount (limited partner) in accordance with article 171 UGB.	Company register Regional courts and the Commercial Court of Vienna	https://justizonline.gv.at/jop/web/firmenbuchabfrage
Limited partnership	42.813		Company register Regional courts and the Commercial Court of Vienna	https://justizonline.gv.at/jop/web/firmenbuchabfrage
Commercial and industrial cooperative societies	1.917	According to the Cooperatives Act (GenG), a commercial and industrial cooperative societyis a legal entity that is itself the holder of rights and obligations. It is an association of persons with legal personality and a non-closed number of members, which essentially serves to promote the interests of its members, such as	Company register Regional courts and the Commercial Court of Vienna	https://justizonline.gv.at/jop/web/firmenbuchabfrage

		credit, purchasing, sales, consumption, utilisation, building, housing and settlement cooperatives. The equity capital is raised by the members by paying in the amount stated in the share.		
European cooperative society	4	The European Cooperative Society (SCE) is a special form of commercial and economic cooperative. It is a legal form with legal personality whose share capital is divided into shares, whereby the number of members and the share capital are variable. Its purpose is to meet the needs of its members and/or to promote their economic and/or social activities; this can be achieved in particular by concluding agreements with its members on the supply of goods or the provision of services or the performance of work within the scope of the activities that the European Cooperative carries out or has carried out. Its internal organisation can be dualistic (executive board and supervisory board) or monistic (administrative board) in accordance with § 22 ff of the SCE Law. There are special requirements for the formation of the European Cooperative Society, as this can only take place through the cross-border	Company register Regional courts and the Commercial Court of Vienna	https://justizonline.gv.at/jop/web/firmenbuchabfrage

		merger of cooperatives or European cooperatives through mergers or conversions.		
European company	15	The European Company (SE) is a special form of Stock corporation whose internal organisation can be dualistic (Management Board and Supervisory Board) or monistic (Administrative Board) in accordance with article 34 of the SE Act. There are special requirements for the formation of an SE, as this can only take place through the cross-border merger of an AG or SE by means of a merger, the formation of a holding SE or a change of legal form.	Company register Regional courts and the Commercial Court of Vienna	https://justizonline.gv.at/jop/web/firmenbuchabfrage
European economic interest groupings	30	The European Economic Interest Grouping is a special partnership which, in accordance with Art. 1 Para. 2 of the EEIG, has the capacity to be the holder of rights and obligations of any kind in its own name, to conclude contracts or perform other legal acts and to stand before the courts. According to Art. 3 Para. 1 EEIG, its purpose is to facilitate or develop the economic activity of its members and to improve or increase the results of this activity; it does not have the purpose of making a profit for itself. Members of a European Economic Interest Grouping can be companies	Company register Regional courts and the Commercial Court of Vienna	https://justizonline.gv.at/jop/web/firmenbuchabfrage

		and other legal entities under public or private law as well as natural persons, whereby a European Economic Interest Grouping must consist of at least two members that have their registered office in different Member States (Art. 4 EEIG).		
Mutual insurance association	10	According to the Insurance Supervision Act 2016 (VAG 2016), a mutual insurance association is an association that insures its members in accordance with the principle of mutuality. A mutual insurance association requires a licence from the FMA to commence business operations in Austria. The name of the association must state that mutual insurance is operated. The associations statutes must be established in the form of a notarial deed. Mutual insurance associations must be entered in the commercial register.	Company register Regional courts and the Commercial Court of Vienna	https://justizonline.gv.at/jop/web/firmenbuchabfrage
Small mutual insurance association	42	This is a mutual insurance association with its registered office in Austria that fulfils the requirements of article 68 (1) or (1a) VAG 2016, has the operation of contract insurance as its object and has only received a licence within the federal territory. A small	Company register/supplementary register Regional courts or Vienna Commercial	https://justizonline.gv.at/jop/web/firmenbuchabfrage https://www.ersb.gv.at

		mutual insurance association can be entered in the commercial register.	Court / Financial Market Authority	
Savings bank	22	Savings banks are legal entities under private law established by municipalities or savings bank associations in accordance with the Savings Bank Act (SpG). They are credit institutions in accordance with the licence granted to them on the basis of the provisions of the Austrian Banking Act (BWG). Savings banks are companies by virtue of their legal form pursuant to article 2 of the Austrian Commercial Code and must be entered in the commercial register.	Company register Regional courts and the Commercial Court of Vienna	https://justizonline.gv.at/jop/web/firmenbuchabfrage
Other legal entity	34	All other legal entities whose entry in the company register is provided for by law in accordance with article 2 no. 13 FBG. As a rule, these are legal entities under public law whose entry in the commercial register is provided for in the law that contains their organisational law.	Company register Regional courts and the Commercial Court of Vienna	https://justizonline.gv.at/jop/web/firmenbuchabfrage
Private foundation	2.973	In accordance with the Private Foundation Act (PSG), a private foundation is a legal entity that is itself the holder of rights and obligations. Assets are dedicated to the private foundation by the founder for the fulfilment of a permitted purpose determined by the founder. The private foundation has no legal	Company register Regional courts and the Commercial Court of Vienna	https://justizonline.gv.at/jop/web/firmenbuchabfrage

		owners and is therefore a foundation within the meaning of Art. 3 no. 6 lit. c of Directive (EU) 2015/849 or pursuant to § 2 no. 3 lit. a WiEReG. A private foundation can be established by one or more founders by means of a notarial deed, whereby at least EUR 70,000 in cash or in kind must be dedicated to the foundation.		
Non-profit foundation or fund established by federal law	308	The charitable foundations and funds are legal entities established in accordance with article 1 (1) of the Federal Foundation and Fund Act 2015 (BStFG 2015) or in accordance with the respective state laws. Pursuant to article 2 (1) BStFG 2015, charitable foundations are assets with legal personality that are permanently dedicated by order of the founder and whose income is used to fulfil charitable or benevolent purposes. Pursuant to article 2 (3) BStFG 2015, charitable funds are assets with legal personality that are not permanently dedicated by order of the founder and that serve to fulfil charitable or benevolent purposes. All charitable provincial foundations and funds are recorded in provincial registers, while federal foundations and funds are recorded in the Federal Register of Foundations and Funds.	Federal Register of Foundations and Funds / Supplementary Register Federal Ministry of the Interior / Registry authority	https://www.bmi.gv.at /409/start.aspx https://www.ersb.gv.at
Non-profit foundation or fund established by state law	302		National register / Supplementary register State authorities / registry authority	Depending on the federal state https://www.ersb.gv.at

Trust	6	A trust is created when a natural or legal person (the settlor) transfers assets, property or rights (the trust assets) to a second person (the trustee), who manages or utilises the transferred assets in the future for one or more third parties (the beneficiaries) in accordance with the rules established by the settlor with effect against anyone. Trusts do not (usually) have their own legal personality; only the trustee has active and passive legal capacity as the owner of the trust assets. Any asset is suitable as the object of a trust, provided it can be owned and is legally transferable. Even if a trust cannot be set up under Austrian law, it could be set up under foreign law and administered from Austria.	Identification number registry authority / registry authority	https://www.ersb.gv.at
Trust-like agreement	0	A trust-like arrangement is another arrangement, such as fiducie, certain types of fiduciary or fideicomisio, provided they are comparable in function or structure to a trust. In principle, trusteeships do not fall under the concept of trust-like agreements, as these are typically not comparable to trusts due to their structure and function. However, if the contractual structure of a trust provides for the management of	Identification number registry authority	https://www.ersb.gv.at

		assets in favour of a person other than the settlor (beneficiary), it must be examined on a case-by-case basis whether an agreement similar to a trust exists.		
Association	134.648	According to article 1 of the Association Act (VerG), an association is a voluntary, permanent association of at least two persons organised on the basis of statutes for the pursuit of a specific, common, idealistic purpose. The association has legal personality (§ 2 Para. 1 VerG). The association's assets may only be used in accordance with the purpose of the association. The members of an association do not necessarily have to contribute capital. The right to form an association is also enshrined in the constitution in article 12 of the Basic Law of 1867. Every association is recorded in the Central Register of Associations and its details can be viewed by the public.	Federal Minister of the Interior / Authorities (indirect federal administration)	https://citizen.bmi.gv.at/at.gv.bmi.fnsweb-p/zvn/public/Registerauszug
Total	406.995			

The following entities have been determined not to be a legal entity, trust or trust-like arrangement:

Name of the unit	Reason for non-inclusion

Corporations under public law	As these cannot have legal owners, the federal government, the federal states, the municipalities and the social insurance institutions are not to be recognised as legal entities.
Fiduciary as nominee agreement	The detailed analysis of trust-like agreements has shown that the trust should be considered a nominee arrangement in accordance with its characteristics and risk profile. If a trust can nevertheless be considered trust-like due to special agreements, this special arrangement is also covered by the scope of application of the Beneficial Owner Registerbeneficial owner register (BOR).

The following legal forms were not included in this risk assessment, as a comprehensive analysis has shown that they cannot be established under Austrian law:

Name	Notes
Trust	The risk of foreign trusts and trust-like agreements was analysed in the risk assessment of foreign legal entities and trusts (2025)
Trust-like agreement	

Transparency of beneficial ownership:
The above-mentioned legal forms are subject to the scope of application of the beneficial owner register act (BORA) in accordance with article 1 (2) BORA and are hereinafter referred to as legal entities. They are obliged to report their beneficial owners to the BORBeneficial Owner Register. In addition, legal entities must review their beneficial owners at least once a year and either confirm that no changes have occurred or report any changes that have been identified. The BOR also contains information on whether the shares in a legal entity are held in the entity's own name or as a trustee for a trustor (nominee agreements). As of 30 September 2024, the reporting rate for legal entities subject to the reporting obligation was 98.34%, the annual review rate was 96.84% and the reporting rate for all legal entities was 94.91%, including legal entities exempt from reporting with automatic data transfer (71.34% of legal entities).

Maintenance of the Beneficial Owner Register:
The Beneficial Owner Register is managed by the registry authority set up within the Federal Ministry of Finance. The responsibilities of the registry authority include professional and technical management, conducting administrative procedures, analysing and reviewing reports, preparing notifications and responding to technical enquiries by telephone and in writing. Ensuring that the data stored in the register is appropriate, accurate and

up-to-date is achieved through a multipronged approach, which includes risk-based supervision. Coercive penalties to enforce the reporting obligation are imposed by the Austrian tax authorities. The Anti-Fraud Office is responsible for penalising breaches of the reporting obligation.

Threat

The threat was assessed on the basis of the three basic scenarios, taking into account the following aspects:

- Threat level based on available statistical data
- Threat level based on an analysis of credible open-source information and the perceptions and opinions of public and private sector experts; and
- Threat scenarios observed for the legal form

The threat assessment is carried out separately for money laundering and terrorism financing and proliferation financing. If there is a threat situation that differs from money laundering and terrorism financing regarding proliferation financing, this is weighted at 20% (40% each for money laundering and terrorism financing).

Legal form	Threat of money laundering	Threat of terrorist financing	Threat Proliferation financing	Remark
Stock corporation	2 - medium	2 - medium	2 - medium	There is no data or observations from experts that indicate a specific threat to stock corporations with regard to **money laundering**. The misuse of stock corporation in the context of various threat scenarios is nevertheless a realistic scenario, meaning that the overall risk is assessed as level 2 - medium. There are no perceptions of **terrorism and proliferation financing** by stock corporations. As the same threat scenarios are relevant as for money laundering, the overall risk is assessed as level 2 - medium.
Limited liability company	3 - high	2 - medium	3 - high	Overall, the threat of Llcs being misused for **money laundering** can be categorised as 3 - High. This is due to observed threats that occur in practice, particularly in the case of limited liability companies, including

				bogus companies or the concealment of beneficial ownership by non-transparent foreign shareholders. In addition, trusteeships and the verification of the origin of funds pose challenges. No specific threat scenarios for **terrorism financing** could be identified. However, as there is also little experience, the overall risk is rated as 2 - medium. As the same threat scenarios are relevant for **proliferation financing** as for money laundering, the risk is also rated as level 3 - high.
Flexible company	3 - high	2 - medium	3 - high	Due to the similarity with the Llc and the fact that no data is yet available, the threat of Flexible companys being misused for **money laundering** or **proliferation financing** is classified as 3 - high. Overall, the threat of flexible companies being misused for **terrorism financing** is classified as 2 - medium, as is the case with limited liability companies.
General partnership	3 - high	2 - medium	2 - medium	Experts report that partnerships do play a role in **money laundering investigations** and that they were also classified as relevant for the identified threat scenarios, which is why the threat was classified as 3 - high. No evidence was found to suggest that partnerships are used for **terrorism financing**, which is why the overall risk is rated as 2 - medium. As relevant threat scenarios for **proliferation financing** can be identified, but these occur less frequently in practice than with limited liability companies, the risk is assessed as 2 - medium.
Limited partnership	3 - high	2 - medium	2 - medium	
Commercial and industrial cooperative societies	1 - low	1 - low	1 - low	There is no practical evidence that commercial cooperatives pose a threat in connection with **money laundering, terrorism financing** or **proliferation financing**, so the risk is classified as 1 - low.

European cooperative society	1 - low	1 - low	1 - low	There are no concrete indications of an increased threat of **money laundering, terrorism financing** or **proliferation financing** in relation to the European legal forms. However, as the same threat scenarios may well be relevant as for the comparable Austrian legal forms, EEIGs and European companies are assessed as medium risk (level 2). European cooperative societys are rated as low risk (level 1).
European company	2 - medium	2 - medium	2 - medium	
European Economic Interest Grouping	2 - medium	2 - medium	2 - medium	
Mutual insurance association	1 - low	1 - low	1 - low	No threats to insurance associations or savings banks in connection with **money laundering, terrorism financing** or **proliferation financing** can be identified. The risk can therefore be assessed as 1 - low.
Small mutual insurance association	1 - low	1 - low	1 - low	
Savings bank	1 - low	1 - low	1 - low	
Other legal entity	1 - low	1 - low	1 - low	As there are no perceptions of threats from **money laundering, terrorism financing** or **proliferation financing** for other legal entities and all experts have assessed the risk as low, the risk is rated as 1 - low.
Private foundation	3 - high	2 - medium	2 - medium	No specific perceptions of private foundations in connection with **money laundering** could be described. However, private foundations can be used to conceal beneficial ownership, as the identified threat scenarios also show. Due to this circumstance, the risk is therefore rated as 3 - high. Although the threat scenarios are also present here, the private foundation was not mentioned by any experts in connection with **terrorism financing** or **proliferation financing**, which is why the risk was therefore assessed as 2 - medium.

Non-profit foundation or fund established by federal law	2 - medium	1 - low	1 - low	Experts have not seen any indications that charitable foundations and funds established under federal and state law could be misused for **money laundering**. However, the registry authority has submitted a suspicious activity report and there is a threat scenario, which is why the threat is rated as 2 - medium. There is no evidence that charitable foundations and funds established under federal and state law are being misused for **terrorism financing** or **proliferation financing**, so the threat is rated as 1 - low.
Non-profit foundation or fund established by state law	2 - medium	1 - low	1 - low	
Association	2 - medium	2 - medium	2 - medium	In practice, there was one specific case in which associations were suspected of being misused for **money laundering**. As no other anomalies were reported and the number of suspicious activity reports is also very low, the risk is categorised as level 2 (medium). The observed threat scenario, in which humanitarian or religious associations in particular serve as a vehicle for transferring funds abroad for the purpose of **terrorism financing**, only affects a very small proportion of all associations, so that the overall risk is assessed as 2 - medium. Although no concrete threats in the area of **proliferation financing** have been perceived, the misuse of associations is conceivable in a similar way to money laundering and the risk is also rated as 2 - medium.

Identified threat scenarios for legal entities:
The following threat scenarios were identified as part of the registry authority's risk-oriented supervision:

Concealment of beneficial ownership through nominee agreements:

One way of concealing beneficial ownership is for one person (nominee/trustee) to hold an interest in a legal entity in their own name but for the account of another person (nominator/trustee). The nominator/trustee can give direct instructions to the nominee/trustee as to how the latter should act as owner. The legal basis for this is a nominee agreement (trust agreement), which can be concluded either in writing or verbally.
The following characteristics have been identified in practice:

1. **Professional nominee agreements:** A lawyer/tax advisor acts as nominee for a client in relation to an investment in a legal entity. A formal nominee agreement (trust agreement) is concluded, which at the same time already provides for an option to transfer the shareholding back to the nominator. This nominee agreement is therefore drawn up by a notary as a notarial deed in order to fulfil the formal requirements for entry in the company register. In such cases, a law or tax consultancy firm or another company owned by a lawyer or tax consultant can also act as nominee.
2. **Informal nominee agreements:** Informal agreements are often used in close family relationships when a person is no longer allowed to act as the owner or director of a legal entity for whatever reason (e.g. insolvency or criminal proceedings). In such cases, the spouse or related parties formally assume the role of owner (nominee) or managing director (nominee director) and act on behalf of the nominator. In such cases, often only a verbal agreement is concluded in reliance on the close family relationship. Such agreements can also be found in connection with the circumvention of sanctions.
3. **Nominee agreement based on factual circumstances:** This type of nominee agreement is frequently observed in connection with dummy companies. People are recruited from (eastern) foreign countries who do not understand the local language or only insufficiently. In some cases, attempts are made to give the appearance of an employment relationship (office work, translation services, visits to authorities). The recruited person is subsequently appointed as managing director and/or shareholder of a legal entity (nominee and/or nominee director) and receives remuneration for this. The nominee then signs the documents required to register the legal entity and set up a bank account. The legal entity is subsequently used for tax and (social) fraud offences, money laundering, etc. The nominator remains in the background and controls the business of the dummy company via the nominee. If the legal entity is identified by the authorities as a bogus company, the nominee is usually faced with high liabilities for tax arrears and high financial penalties, while the nominator will often remain undetected. If the nominee realises that it is working for a sham company, it is often intimidated by threats and coercion to the extent that it continues in its role as nominee and/or nominee director.

However, nominee agreements can also occur in practice with foundations. In this case, the nominee acts as the founder and sets up a (private) foundation in his own name for a nominator (trustee). The nominator does not appear in the foundation and the nominee effectively donates the assets that he has previously received in trust from the nominator. The nominator does not initially appear before the foundation, but can exercise all founder rights via the nominee on the basis of a contractual agreement. As high assets are regularly involved, lawyers or tax advisors or related parties are used

for this threat scenario. If the nominator wishes his assets to be paid out, he can appoint himself or persons close to him as beneficiaries via the nominee. Comparable constructions are also conceivable with trusts or trust-like agreements.

Bogus company

The use of limited liability companies to conceal the origin of financial resources was already described in the 2021 National Risk Assessment. Several companies (or shell companies purchased specifically for this purpose) are used to channel financial flows along the constructed company chain. Fictitious managing directors from abroad (usually from Eastern European countries) are used for the companies involved, who are also entered in the company register as shareholders in order to conceal the identity of the controlling persons. There is therefore often an overlap with the "concealment of beneficial ownership through nominee agreements". Other bogus companies or foreign legal entities can also act as owners. However, the key feature here is also a fictitious managing director who generally has no insight into the business activities and is supported by another person at appointments who, for example, poses as an interpreter.
The legal entities concerned are usually active in the construction industry or in trade, particularly within Europe, and are linked to each other by orders or fictitious invoices. The funds forwarded in this way are ultimately settled in cash. These dummy companies often issue fictitious invoices to active commercial companies, which are then settled in cash via the fictitious company and returned to the companies minus a discount. These companies then receive cash, which can be used to pay employees, for example, by circumventing social security and income tax regulations (undeclared payment).
It is characterised by the fact that another person is often present during cash withdrawals by the managing director to supervise the fictitious managing director. Many of the intermediary companies have employees, at least for a short time, whereby social fraud and the subsequent insolvency of individual companies typically occur.
Limited liability companies are attractive for this threat scenario because the legal form is particularly suitable for quick company takeovers. Existing companies (shelf companies or shell companies) are also frequently used for these purposes. The advantage of such shelf companies is that they are quickly available when needed. In addition, the longer period of existence can convey seriousness and legitimacy when entering into a business relationship, for example with a bank.

Private foundations without declared beneficiaries
The beneficiaries of a private foundation are those persons who may receive benefits from the private foundation or those who are to receive any assets remaining after the liquidation of the private foundation. The beneficiaries must be reported by the private foundation to the BORBeneficial Owner Register if they are natural persons (from 1 December 2025 also legal entities). The tax office for large companies must be informed of all beneficiaries (natural persons and legal entities) electronically without delay.

As the beneficiaries should ultimately receive the assets of the private foundation, it is essential to identify and verify the beneficiaries as part of the customer due diligence of private foundations.
There may also be good reasons why no beneficiaries were reported:

- The purpose of the foundation suggests that there are no specific beneficiaries. Examples are charitable purposes, preservation of historical buildings owned by the foundation, provision for family members not yet born
- The private foundation was established less than five years ago and it is obvious that the founder is not dependent on benefits from the private foundation due to other sources of income.
- The founder is also the foundation's board member and therefore cannot yet be appointed as a beneficiary (note: this could also be an indication of a trust foundation)

Circumvention of financial sanctions

With regard to the sanctions imposed by the EU Commission due to the Russian war of aggression against Ukraine and other crises, the potential circumvention of sanctions was identified as a threat scenario. The focus of this threat scenario is the circumvention of financial sanctions by concealing beneficial ownership. It is often the case that sanctioned persons acted as beneficial owners before they were sanctioned and that the ownership structure changed before or after the sanctions were imposed. Beneficial ownership can be concealed by using domestic legal entities or complex foreign shareholding structures.
Threats to domestic legal entities:

- Nominee agreements
- Trust foundations

Threats from foreign ownership structures

- Nominee agreements with foreign parent entities domiciled in jurisdictions with limited transparency
- Use of non-transparent foreign legal entities, such as trusts

Use of associations for the purposes of terrorism financing

A threat scenario was already identified in the 2021 National Risk Assessment that describes associations as possible vehicles for transferring funds abroad for the purpose of terrorism financing. In the NPO 2024 sectoral risk assessment, this risk was analysed in detail and the risk was considered in

relation to several criteria. The sectoral risk assessment concludes that although there is a threat in principle, the risk is classified as low. The legal entities concerned are organisations that have been in existence for several years or decades, which supposedly pursue humanitarian or charitable goals, but the funds raised abroad do not reach the advertised aid projects, or only in part. Recipients of payments are often natural persons or foreign organisations in countries severely affected by terrorism, whereby the use of the funds cannot be verified due to a lack of evidence or records. In addition, national charities working as aid organisations in crisis regions can be misused, as they make use of local helpers whose background cannot be extensively clarified. As only a very small part (approx. 0.06%) of the sector is affected by this threat scenario, as shown in detail in the NPO sectoral risk assessment, no increased threat can be derived for the entire legal form of association.

Conclusion: In summary, the threat for all legal forms is classified as 2.65 - high for money laundering, 1.99 - medium for terrorism financing and 2.49 - medium for proliferation financing.

Vulnerability

The baseline scenarios were used to assess the vulnerability of all legal forms with regard to misuse for the purposes of financing terrorism or proliferation and money laundering. The corresponding results are shown for each legal form. Where differences exist with regard to money laundering or the financing of terrorism or proliferation, these are shown separately.

(a) Risk potential:

Size of the sector

The greater the economic significance of a particular legal form, the greater the extent of the potential risk exposure. The risk was assessed as follows:

Legal form	Number and resulting risk	Evaluation of growth	Amount of assets held	Risk from the size of the sector
Stock corporationStock corporation	891 1 - low	1 - low	4 - very high	2 - medium
Limited liability company	201.625	2- medium	3 - high	3 - high

	4 - very high			
Flexible companyFlexible company	762 1 - low	1 - low	1 - low	1 - low
General Partnership	22.139 2 - medium	2 - medium	2 - medium	2 - medium
Limited partnership	42.813 2 - medium	1 - low	2 - medium	1.67 - medium
Commercial and industrial cooperative societies	1.917 1 - low	2 - medium	1 - low	1.33 - low
European cooperative society	4 1 - low	2 - medium	1 - low	1.33 - low
European company	15 1 - low	2 - medium	1 - low	1.33 - low
European Economic Interest Grouping	30 1 - low	2 - medium	1 - low	1.33 - low
Mutual insurance association	10 1 - low	1 - low	1 - low	1 - low
Small mutual insurance association	42 1 - low	1 - low	1 - low	1 - low
Savings bank	22 1 - low	1 - low	2 - medium	1.33 - low
Other legal entity	34 1 - low	1 - low	1 - low	1 - low

Private foundation	2.973 1 - low	1 - low	4 - very high	2 - medium
Non-profit foundation or fund established by federal lawNon-profit foundation or fund established by federal law	308 1 - low	2 - medium	1 - low	1.33 - low
Non-profit foundation or fund established by state law foundation or fund	302 1 - low	1 - low	1 - low	1 - low
Association	136.056 3 - high	2 -medium	1 - low	2 - medium

Type of business risk

The risk and risk potential increases if a legal form is increasingly active in economic sectors that have an increased risk with regard to money laundering. A list of high-risk economic sectors was drawn up as part of the methodology. Based on a quantitative analysis, the proportion of the legal form was compared with the average proportion (24.16%). This enabled the following risk to be determined:

Legal form	Share of risky industries	Risk	Legal form	Share of risky industries	Risk
Stock corporation	35,35%	3 - high	Mutual insurance association	36,36%	3 - high
Limited liability company	36,66%	3 - high	Small mutual insurance association	0,00%	1 - low
Flexible company	19,42%	2 - medium	Savings bank	100%	4 - very high

General Partnership	26,52%	3 - high	Other legal entity	5,88%	2 - medium
Limited partnership	35,25%	3 - medium	Private foundation	97,34	4 - very high
Commercial and industrial cooperative societies	22,43%	2 - medium	Non-profit foundation or fund established by federal lawNon-profit foundation or fund established by federal law	0,65%	1 -low
European cooperative society	0,00%	1 - low	Non-profit foundation or fund established by state law foundation or fund	0,99%	1 - low
European company	33,33%	3 - high	Association	0,24%	1 - low
European Economic Interest Grouping	20,00%	2 - medium			

Geographical and cross-border risk exposure

Cross-border ownership and activities of legal entities increase vulnerability to ML/TF/PF. Vulnerability is also increased when legal entities are linked to offshore jurisdictions and other "favoured" locations for opaque offshore structures or are controlled by management, legal or beneficial owners with a connection to such high ML/TF/PF risk countries (domicile, residence and nationality). A purely quantitative analysis was carried out, whereby the individual categories by risk and the share of third countries were weighted at 25% and the share of high-risk countries at 75% and compared with the average share (1.38%).

Legal form	Weighted average of third countries and risk countries	Risk	Legal form	Weighted average of third countries and risk countries	Risk

Stock corporation	1,83%	2 - medium	Mutual insurance association	0,00%	1 - low
Limited liability company	1,56%	2 - medium	Small mutual insurance association	0,00%	1 - low
Flexible company	1,39%	2 - medium	Savings bank	0,00%	1 - low
General Partnership	1,62%	2 - medium	Other legal entity	0,40%	1 - low
Limited partnership	2,05%	3 - high	Private foundation	0,80%	2 - medium
Commercial and industrial cooperative societies	0,01%	1 - low	Non-profit foundation or fund established by federal lawNon-profit foundation or fund established by federal law	0,54%	2 - medium
European cooperative society	0,68%	2 - medium	Non-profit foundation or fund established by state law foundation or fund	0,14%	1 - low
European company	4,41%	3 - medium	Association	0,34%	1 - low
European Economic Interest Grouping	1,13%	2 - medium			

(b) legal framework and supervision/governance:

Risk of concealment through nominee agreements and bearer shares

The beneficial ownership of legal entities can be concealed using various instruments. Nominees, nominee directors, in particular informal nominees (or "straw men") and bearer shares and bearer share warrants represent a significant vulnerability. Therefore, a qualitative and quantitative analysis

(comparison with the average of reported nominee agreements 0.49%) was used to assess how the beneficial ownership of legal forms can be concealed, with only the higher risk being assessed in each case.

Legal form	Nominee agreement legally permissible	Share of reported nominee agreements		Risk from bearer shares	Risk of concealment
		Share	Risk		
Stock corporation	Yes / 3 - high	1,01%	4 - high	2 - medium	3.5 - very high
Limited liability company	Yes / 3 - high	0,83%	3 - high	1 - low	3 - high
Flexible company	Yes / 3 - high	0,26%	2 - medium	1 - low	2.5 - high
General Partnership	Yes / 3 - high	0,11%	2 - medium	1 - low	2.5 - high
Limited partnership	Yes / 3 - high	0,50%	3 - high	1 - low	3 - high
Commercial and industrial cooperative societies	Yes / 3 - high	0,00%	1 - low	1 - low	2 - medium
European cooperative society	Yes / 3 - high	0,00%	1 - low	1 - low	2 - medium
European company	Yes / 3 - high	0,00%	1 - low	3 - high	3 - high
European Economic Interest Grouping	Yes / 3 - high	0,00%	1 - low	1 - low	2 - medium
Mutual insurance association	No / 1 - low	0,00%	1 - low	1 - low	1 - low
Small mutual insurance association	No / 1 - low	0,00%	1 - low	1 - low	1 - low
Savings bank	No / 1 - low	0,00%	1 - low	1 - low	1 - low

Other legal entity	No / 1 - low	0,00%	1 - low	1 - low	1 - low
Private foundation	Yes / 3 - high	1,08%	4 - very high	1 - low	3.5 - very high
Non-profit foundation or fund established by federal law	Yes / 3 - high	0,00%	1 - low	1 - low	2 - medium
Non-profit foundation or fund established by state law foundation or fund	Yes / 3 - high	0,99%	3 - high	1 - low	3 - high
Association	Yes / 3 - high	0,00%	1 - low	1 - low	2 - medium

Simplicity, speed and costs of founding/registering legal entities

The suitability of certain legal forms for abuse for money laundering and terrorism financing can vary considerably depending on the specific legal requirements for the establishment and registration of a legal form. In general, the lower the requirements for establishing a legal entity, the lower the number of persons involved, the easier it is to transfer shares, the lower the costs and the quicker and easier it is to establish, the higher the risk for this legal entity.

Legal form	Requirements for the foundation	Number of persons involved	Legal requirements for the transfer of company shares	Economic costs of formation, registration and change of ownership	Simplicity and speed of incorporation and registration	Risk of vulnerability
Stock corporation	1	1	2	1	2	1.4 - low
Limited liability company	1	4	1	2	3	2.2 - medium
Flexible company	1	4	2	2	3	2.4 - medium

General Partnership	2	4	3	3	3	3 - high
Limited partnership	2	4	3	3	3	3 - high
Commercial and industrial cooperative societies	2	3	3	3	1	2.6 - high
European cooperative society	The risk assessment of the comparable domestic legal form (commercial and industrial cooperative society) was taken as the basis and adjusted by -0.2 levels to take account of the higher capital requirements.					2.2 - medium
European company	The risk assessment of the comparable domestic legal form (stock corporation) was taken as the basis and adjusted by -0.2 levels to take account of the higher capital requirements.					1.2 - low
European Economic Interest Grouping	The risk assessment of the comparable domestic legal form (general partnership) was taken as the basis and adjusted by -0.4 levels to take into account the higher capital requirements and the higher formal requirements with regard to the articles of association.					2.6 - high
Mutual insurance association	1	2	1	1	1	1.2 - low
Small mutual insurance association	1	2	1	1	1	1.2 - low
Savings bank	1	2	1	1	1	1.2 - low
Other legal entity	1	1	1	1	1	1 - low
Private foundation	1	2	1	1	2	1.4 - low
Non-profit foundation or fund established by federal law	2	2	3	1	1	1.6 - medium

Non-profit foundation or fund established by state law foundation or fund	2	2	3	1	1	1.6 - medium
Association	4	3	3	4	3	3.4 - high

Attractiveness of a legal form for money laundering and terrorism financing (ongoing activities)

The suitability of certain legal forms for abuse for the financing of terrorism and proliferation and for money laundering can vary significantly depending on the specific legal requirements and economic conditions for the ongoing operation of a legal entity.

Legal form	Residency requirement	Economic costs of going concern and internal governance	Protective measures in the event of insolvency	Fiscal attractiveness	Risk of vulnerability
Stock corporation	3	1	1	1	1.5 - medium
Limited liability company	3	3	1	1	2 - medium
Flexible company	3	3	1	1	2 - medium
General Partnership	3	4	1	2	2.5 - high
Limited partnership	3	4	1	2	2.5 - high
Commercial and industrial cooperative societies	3	2	1	2	2 - medium
European cooperative society	3	2	1	2	2 - medium
European company	3	1	1	1	1.5 - medium

European Economic Interest Grouping	3	4	1	2	2.5 - high
Mutual insurance association	3	1	1	1	1.5 - medium
Small mutual insurance association	3	2	1	2	2 - medium
Savings bank	3	1	1	1	1.5 - medium
Other legal entity	n.a. as the requirements for each other legal entity are defined individually in the Establishment Act.				2.00 - medium
Private foundation	2	1	1	3	1.75 - medium
Non-profit foundation or fund established by federal law	3	1	1	3	2.00 - medium
Non-profit foundation or fund established by state law foundation or fund	3	1	1	3	2.00 - medium
Association	3	3	1	3	2.5 - high

Availability of basic information on legal entities and degree of information accuracy

The suitability of certain legal forms for abuse for the financing of terrorism and proliferation and for money laundering may vary significantly depending on the specific legal requirements in terms of transparency and accessibility of basic information of a legal form.

Legal form	Completeness of the basic information	Accuracy and quality of basic information	Public access to basic information	Risk of vulnerability
Stock corporation	2	3	3	2.67 -high

Limited liability company	1	3	1	1.67 - medium
Flexible company	2	3	2	2.33 - medium
General Partnership	3	3	3	3 - high
Limited partnership	3	3	3	3 - high
Commercial and industrial cooperative societies	1	3	2	2 -medium
European cooperative society	1	3	2	2 -medium
European company	2	3	3	2.67 -high
European Economic Interest Grouping	3	3	3	3 - high
Mutual insurance association	2	3	1	2 - medium
Small mutual insurance association	2	2	1	1.67 - medium
Savings bank	2	3	1	2 - medium
Other legal entity	1	3	1	1.67 - medium
Private foundation	3	3	2	2.67 - high
Non-profit foundation or fund established by federal law	1	3	2	2 - medium
Non-profit foundation or fund established by state law foundation or fund	1	3	2	2 - medium
Association	1	3	1	1.67 - medium

Availability of adequate, accurate and up-to-date information on the beneficial owners of the legal entities

The suitability of certain legal forms for abuse for the financing of terrorism and proliferation and for money laundering may vary significantly depending on the availability of adequate, accurate and up-to-date information on the beneficial owners. The following parameters were quantitatively assessed: entities with no reported beneficial owner, entities that have not updated their BOs annually, and entities that have not remedied a remark within six weeks.

Legal form	Legal entities without reported beneficial ownership		Legal entities that have not performed an annual update		Legal entities that have not rectified a remark within six weeks		Risk of vulnerability	Notes
	Share	Risk	Share	Risk	Share	Risk		
Stock corporation	1,12%	2 - medium	3,03%	3 - high	0,00%	1 - low	2 - medium	
Limited liability company	0,51%	2 - medium	1,17%	2 - medium	0,06%	1 - low	1.67 - medium	
Flexible company	3,41%	3 - high	0,00%	2 - medium*	0,00%	1 - low	2 - medium	*As no meaningful data was available at the time of the analysis, the rating is 2 - medium
General Partnership	0,20%	1 - low	0,21%	1 - low	0,01%	1 - low	1 - low	
Limited partnership	0,87%	2 - medium	1,06%	2 - medium	0,04%	1 - low	1.67 - low	
Commercial and industrial cooperative societies	2,45%	2 - medium	0,05%	1 - low	0,00%	1 - low	1.33 - low	

European cooperative society	0,00%	1 - low	0,00%	1 - low	0,00%	1 - low	1 - low	
European company	0,00%	1 - low	0,00%	1 - low	0,00%	1 - low	1 - low	
European Economic Interest Grouping	26,67%	4 - very high	16,67%	4 - very high	0,00%	1 - low	3 - high	
Mutual insurance association	9,09%	3 - high	0,00%	1 - low	0,00%	1 - low	1.67 - medium	
Small mutual insurance association	0,00%	1 - low	0,00%	1 - low	0,00%	1 - low	1 - low	
Savings bank	0,00%	1 - low	0,00%	1 - low	0,00%	1 - low	1 - low	
Other legal entity	0,00%	1 - low	11,76%	4 - very high	0,00%	1 - low	2.00 - medium	
Private foundation	1,28%	2 - medium	2,05%	2 - medium	0,13%	2 - medium	2.00 - medium	
Non-profit foundation or fund established by federal law	2,92%	3 - high	9,42%	3 - high	0,00%	1 - low	2.33 - medium	
Non-profit foundation or fund established by state law foundation or fund	0,99%	2 - medium	6,29%	3 - high	0,00%	1 - low	2 - medium	
Association	13,02%	4 - very high	0,00%	1 - low	0,00%	1 - low	2 - medium	

Complexity of the ownership and control structure

The availability of adequate information on beneficial ownership can be impaired by a complex ownership and control structure. Therefore, the proportion (average 2.26%) of non-transparent foreign ultimate legal entities (foundations, trusts and trust-like legal arrangements) and the proportion (average 0.08%) of subsidiary reports where no beneficial owners could be identified after exhausting all possibilities were be analysed and evaluated.

Legal form	Non-transparent foreign top-level legal entities		Subsidiary notifications after all possibilities have been exhausted		Risk of vulnerability	Remarks
	Share	Risk	Share	Risk		
Stock corporation	7,60%	3 - high	1,23%	4 - very high	3.5 - very high	
Limited liability company	2,40%	2 - medium	0,14%	3 - high	2.5 - high	
Flexible company	0,00%	1 - low	0,00%	1 - low	1 - low	
General Partnership	0,89%	1 - low	0,03%	2 - medium	1.5 - medium	
Limited partnership	1,48%	2 - medium	0,05%	2 - medium	2 - medium	
Commercial and industrial cooperative societies	-	1 - low	0,16%	3 - high	2 - medium	
European cooperative society	-	1 - low	0,00%	3 - high	2 - medium	
European company	11,76%	4 - high	0,00%	1 - low	2.5 - high	
European Economic Interest Grouping	14,29%	4 - high	0,00%	1 - low	2.5 - high	

Mutual insurance association	-	1 - low	0,00%	1 - low	1 - low	(Small) mutual insurance associations and savings banks have no ultimate legal entity, so that no complex ownership structures can arise.
Small mutual insurance association	-	1 - low	0,00%	1 - low	1 - low	
Savings bank	-	1 - low	0,00%	1 - low	1 - low	
Other legal entity	-	1 - low	2,94%	4 - very high	2.5 - high	The high figure for subsidiary declarations where all possibilities have been exhausted is probably due to an incorrect legal interpretation on the part of the legal entities concerned.
Private foundation	-	3 - high	0,00%	-	3 - high	Private foundations have no ultimate legal entity and there is no provision for subsidiary reporting. However, legal entities or other private foundations can be founders or beneficiaries, which can result in very complex ownership structures in practice.
Non-profit foundation or fund established by federal law	-	1 - low	0,00%	1 - low	1 - low	Non-profit foundations or funds established under federal or state law do not have an ultimate legal entity. No complex structures have been observed in practice.
Non-profit foundation or fund established by state law foundation or fund	-	1 - low	0,00%	1 - low	1 - low	
Association	0,00%	1 - low	0,00%	1 - low	1 - low	

(c) Risk awareness:

The suitability of certain legal entities for the financing of terrorism and proliferation and for money laundering can vary considerably depending on the quality of the measures taken by obliged entities. The degree of risk awareness of the obliged entities with regard to the respective legal forms is decisive in determining whether sufficient measures are taken. An assessment was made of the individual professional groups based on the Fourth Round Mutual Evaluation Report[5] and the FATF's first[6] and second[7] follow-up report, which suggests a medium level of risk awareness. If there are deviations specific to the legal form, these are dealt with in more detail in the risk assessment specific to the legal form. The risk of insufficient measures being taken by obliged entities due to insufficient risk awareness was therefore assessed.

Legal form	Risk that insufficient measures are taken	Legal form	Risk that insufficient measures are taken
Stock corporation	2 - medium	Mutual insurance association	2 - medium
Limited liability company	2 - medium	Small mutual insurance association	2 - medium
Flexible company	3 - high	Savings bank	2 - medium
General Partnership	2 - medium	Other legal entity	2 - medium
Limited partnership	2 - medium	Private foundation	2 - medium

[5] See FATF (2016), Anti-money laundering and counter-terrorist financing measures - Austria, Fourth Round Mutual Evaluation Report, FATF, Paris, www.fatf-gafi.org/publications/mutualevaluations/documents/mer-austria-2016.html and

[6] See FATF (2017), Anti-money laundering and counter-terrorist financing measures - Austria, 1st Enhanced Follow-up Report &Technical Compliance Re-Rating, FATF, Paris, www.fatf-gafi.org/publications/mutualevaluations/documents/fur-austria-2017.html

[7] See FATF (2018), Anti-money laundering and counter-terrorist financing measures - Austria, 2nd Enhanced Follow-up Report & Technical Compliance Re-Rating, FATF, Paris, http://www.fatf-gafi.org/publications/mutualevaluations/documents/fur-austria-2018.html

Commercial and industrial cooperative societies	2 - medium	Non-profit foundation or fund established by federal law	2 - medium
European cooperative society	3 - high	Non-profit foundation or fund established by state law foundation or fund	2 - medium
European company	3 - high	Association	2 - medium
European Economic Interest Grouping	3 - high		

Terrorism financing

The analysis of the misuse of legal entities with regard to terrorism financing is generally identical to the previous analysis for money laundering. The following section therefore only deals with aspects in which there are differences.

Type of business risk

The risk and risk potential increases if a legal form is increasingly active in economic sectors that have an increased risk with regard to terrorism financing. A list of high-risk economic sectors was drawn up as part of the methodology. Based on a quantitative analysis, the proportion of the legal form was compared with the average proportion (24.16%). This enabled the following risk to be determined:

Legal form	Share of risky industries	Risk	Legal form	Share of risky industries	Risk
Stock corporation	20,20%	2 - medium	Mutual insurance association	0,00%	1 - low
Limited liability company	11,39%	2 - medium	Small mutual insurance association	0,00%	1 - low

Flexible company	7,09%	2 - medium	Savings bank	100%	4 - very high
General Partnership	5,80%	2 - medium	Other legal entity	0,00%	1 - low
Limited partnership	8,53%	32- medium	Private foundation	0,03%	1 - low
Commercial and industrial cooperative societies	17,11%	2 - medium	Non-profit foundation or fund established by federal law	0,00%	1 -low
European cooperative society	0,00%	1 - low	Non-profit foundation or fund established by state law foundation or fund	0,66%	1 - low
European company	13,33%	2 - medium	Association	0,10%	1 - low
European Economic Interest Grouping	16,67%	2 - medium			

Geographical and cross-border risk exposure

Cross-border ownership and activities of legal entities increase vulnerability to TF. Vulnerability is also increased when legal entities are linked to offshore jurisdictions and other "favourite" locations for opaque offshore structures or are controlled by management, legal or beneficial owners with a link to such high ML/TF risk countries (domicile, residence and nationality). A purely quantitative analysis was carried out, whereby the individual categories by risk and the share of third countries were weighted at 25% and the share of high-risk countries at 75% and compared with the average share (1.02%).

Legal form	Weighted average of third countries and risk countries	Risk	Legal form	Weighted average of third countries and risk countries	Risk

Stock corporation	1,59%	2 - medium	Mutual insurance association	0,00%	1 - low
Limited liability company	1,06%	2 - medium	Small mutual insurance association	0,00%	1 - low
Flexible company	1,24%	2 - medium	Savings bank	0,00%	1 - low
General Partnership	1,19%	2 - medium	Other legal entity	0,40%	1 - low
Limited partnership	1,80%	2 - medium	Private foundation	0,58%	2 - medium
Commercial and industrial cooperative societies	0,01%	1 - low	Non-profit foundation or fund established by federal law	0,22%	1 - low
European cooperative society	0,68%	2 - medium	Non-profit foundation or fund established by state law foundation or fund	0,16%	1 - low
European company	4,55%	3 - high	Association	0,25%	2 - low
European Economic Interest Grouping	1,13%	2 - medium			

Proliferation financing

The analysis of the misuse of legal entities with regard to proliferation financing is generally identical to the previous analysis for money laundering. The following therefore only deals with aspects in which there are differences.

Type of business risk

The risk and risk potential increases if a legal form is increasingly active in economic sectors that have an increased risk with regard to proliferation financing. A list of high-risk economic sectors was drawn up as part of the methodology. Based on a quantitative analysis, the share of the legal form was compared with the average share (7.11%). This enabled the following risk to be determined:

Legal form	Share of risky industries	Risk	Legal form	Share of risky industries	Risk
Stock corporation	19,08%	2 - medium	Mutual insurance association	0,00%	1 - low
Limited liability company	10,57%	2 - medium	Small mutual insurance association	0,00%	1 - low
Flexible company	6,56%	2 - medium	Savings bank	100%	4 - very high
General Partnership	4,82%	2 - medium	Other legal entity	0,00%	1 - low
Limited partnership	7,39%	32- medium	Private foundation	0,03%	1 -low
Commercial and industrial cooperative societies	17,01%	2 - medium	Non-profit foundation or fund established by federal law	0,00%	1 -low
European cooperative society	0,00%	1 - low	Non-profit foundation or fund established by state law foundation or fund	0,66%	1 - low
European company	13,33%	2 - medium	Association	0,10%	1 - low
European Economic Interest Grouping	16,67%	2 - medium			

Geographical and cross-border risk exposure

Cross-border ownership and activities of legal entities increase vulnerability to PF. Vulnerability is also increased when legal entities are linked to offshore jurisdictions and other "favourite" locations for opaque offshore structures or are controlled by management, legal or beneficial owners with a connection to such high PF risk countries (domicile, residence and nationality). A purely quantitative analysis was carried out, whereby the individual categories by risk and the share of third countries were weighted at 25% and the share of high-risk countries at 75% and compared with the average share (0.97%).

Legal form	Weighted average of third countries and risk countries	Risk	Legal form	Weighted average of third countries and risk countries	Risk
Stock corporation	1,40	2 - medium	Mutual insurance association	0,00	1 - low
Limited liability company	1,07	2 - medium	Small mutual insurance association	0,00	1 - low
Flexible company	1,01	2 - medium	Savings bank	0,00	1 - low
General Partnership	1,18	2 - medium	Other legal entity	0,40	1 - low
Limited partnership	1,74	2 - medium	Private foundation	0,66	2 - medium
Commercial and industrial cooperative societies	0,01	1 - low	Non-profit foundation or fund established by federal law	0,23	1 - low
European cooperative society	0,68	2 - medium	Non-profit foundation or fund established by state law foundation or fund	0,14	1 - low

European company	3,10	3 - high	Association	0,24	1 - low
European Economic Interest Grouping	1,09	2 - medium			

<u>Conclusion</u>: In summary, the vulnerability for all legal forms for money laundering is rated at 2.20 - medium, and for terrorist financing and proliferation financing at 2.12 - medium in each case.

Risk-minimizing measures

Risk mitigation measures can reduce the likelihood that the identified threats and the associated vulnerability will have consequences.
The assessment of the quality of the risk mitigation measures aims to determine the strength of existing risk mitigation measures, whereby the maximum strength of the risk mitigation measures was assumed to be one.

Legal form	Enforcement of the obligation to submit a declaration after the establishment of a legal entity or after an annual review by means of an automatic penalty procedure		Mandatory inspection for obliged entities when establishing a business relationship combined with the obligation to make a note of incorrect reports		Risk-oriented analysis and review of incoming notifications by the registry authority		Effectiveness of the national and international exchange of information		Total amount of the risk-minimising effect
	Effect	Reduction	Effect	Reduction	Effect	Reduction	Effect	Reduction	
Stock corporation	strong	-0,3	strong	-0,3	strong	-0,3	strong	-0,1	-1
Limited liability company	strong	-0,3	strong	-0,3	strong	-0,3	strong	-0,1	-1
Flexible company	strong	-0,3	strong	-0,3	strong	-0,3	strong	-0,1	-1
General Partnership	strong	-0,3	strong	-0,3	strong	-0,3	strong	-0,1	-1

Limited partnership	strong	-0,3	strong	-0,3	strong	-0,3	strong	-0,1	-1
Commercial and industrial cooperative societies	strong	-0,3	strong	-0,3	strong	-0,3	strong	-0,1	-1
European cooperative society	strong	-0,3	strong	-0,3	strong	-0,3	strong	-0,1	-1
European company	strong	-0,3	strong	-0,3	strong	-0,3	strong	-0,1	-1
European Economic Interest Grouping	strong	-0,3	strong	-0,3	strong	-0,3	strong	-0,1	-1
Mutual insurance association	strong	-0,3	strong	-0,3	strong	-0,3	strong	-0,1	-1
Small mutual insurance association	strong	-0,3	strong	-0,3	strong	-0,3	strong	-0,1	-1
Savings bank	strong	-0,3	strong	-0,3	strong	-0,3	strong	-0,1	-1
Other legal entity	strong	-0,3	strong	-0,3	strong	-0,3	strong	-0,1	-1
Private foundation	strong	-0,3	strong	-0,3	strong	-0,3	strong	-0,1	-1
Non-profit foundation or fund established by federal law	Satisfactory	-0,2	strong	-0,3	strong	-0,3	strong	-0,1	-0,9
Non-profit foundation or fund established by state law foundation or fund	Satisfactory	-0,2	strong	-0,3	strong	-0,3	strong	-0,1	-0,9
Association	strong	-0,3	strong	-0,3	strong	-0,3	strong	-0,1	-1

Total risk

Calculation method: 40% threat + 60% vulnerability - risk-reducing measures = total risk.

	Threat			Vulnerability			Inherent Risk			Risk minimisation measures	Total risk		
	ML	TF	PF	ML	TF	PF	ML	TF	PF		ML	TF	PF
Stock corporation	2,00	2,00	2,00	2,31	2,11	2,11	2,18	2,06	2,06	1,00	**1,18**	**1,06**	**1,06**
Limited liability company	3,00	2,00	3,00	2,22	2,12	2,12	2,53	2,07	2,47	1,00	**1,53**	**1,07**	**1,47**
Flexible company	3,00	2,00	3,00	2,22	2,22	2,22	2,53	2,13	2,53	1,00	**1,53**	**1,13**	**1,53**
General partnership	3,00	2,00	2,00	2,20	2,10	2,10	2,52	2,06	2,06	1,00	**1,52**	**1,06**	**1,06**
Limited partnership	3,00	2,00	2,00	2,38	2,18	2,18	2,63	2,11	2,11	1,00	**1,63**	**1,11**	**1,11**
Commercial and industrial cooperative societies	1,00	1,00	1,00	1,81	1,81	1,81	1,48	1,48	1,48	1,00	**0,48**	**0,48**	**0,48**
European cooperative society	1,00	1,00	1,00	1,82	1,82	1,82	1,49	1,49	1,49	1,00	**0,49**	**0,49**	**0,49**
European company	2,00	2,00	2,00	2,04	1,94	1,94	2,02	1,96	1,96	1,00	**1,02**	**0,96**	**0,96**
European economic interest grouping	2,00	2,00	2,00	2,61	2,61	2,61	2,37	2,37	2,37	1,00	**1,37**	**1,37**	**1,37**
Mutual insurance association	1,00	1,00	1,00	1,60	1,40	1,40	1,36	1,24	1,24	1,00	**0,36**	**0,24**	**0,24**
Small mutual insurance association	1,00	1,00	1,00	1,29	1,29	1,29	1,17	1,17	1,17	1,00	**0,17**	**0,17**	**0,17**
Savings bank	1,00	1,00	1,00	1,60	1,60	1,60	1,36	1,36	1,36	1,00	**0,36**	**0,36**	**0,36**
Other legal entity	1,00	1,00	1,00	1,60	1,50	1,50	1,36	1,30	1,30	1,00	**0,36**	**0,30**	**0,30**
Private foundation	3,00	2,00	2,00	2,27	1,97	1,97	2,56	1,98	1,98	1,00	**1,56**	**0,98**	**0,98**
Non-profit foundation or fund established by federal law	2,00	1,00	2,00	1,93	1,83	1,83	1,96	1,50	1,90	0,90	**1,06**	**0,60**	**1,00**
Non-profit foundation or fund established by state law	2,00	1,00	2,00	1,76	1,76	1,76	1,86	1,46	1,86	0,90	**0,96**	**0,56**	**0,96**
Association	2,00	2,00	2,00	1,89	1,89	1,89	1,93	1,93	1,93	1,00	**0,93**	**0,93**	**0,93**
Total	**2,65**	**1,99**	**2,49**	**2,12**	**2,05**	**2,05**	**2,34**	**2,03**	**2,22**	**1,00**	**1,34**	**1,03**	**1,22**

*Total risk = average value weighted by number of legal entities per legal form

Recommendations

With regard to the threat scenario of **concealment of beneficial ownership through nominee agreements**, it is recommended to pay attention to the following risk factors:

- Lawyers, tax advisors or other professional party representatives as owners of legal entities or in the exercise of functions in foundations and trusts (founder, settlor or beneficiary)
- Persons are appointed as beneficiaries who obviously have no connection to the founder (e.g. different nationality or residence in another country)
- Persons as managing directors or owners of legal entities who obviously have no knowledge of the business processes and are supported or "represented" before authorities and obliged entities by persons close to them
- Persons registered as managing directors (and shareholders) who are accompanied by a chaperone when dealing with authorities or banks (especially cash withdrawals).

and the following test steps:

- Examination of the source of funds of a private foundation, in particular whether the financial circumstances of the founder match the foundation capital contributed.
- If the founders' reported shares do not total 100% due to endowments from other persons who were not reported as founders, the origin of the foundation's funds should be examined more closely and, in particular, the economic and personal reason for the endowments should be ascertained and assessed.

With regard to the threat scenario of **bogus companies**, it is recommended to pay attention to the following risk factors:

- Legal entity was founded less than one year ago or there has been a change of shareholder in the last year
- The same person is a shareholder and managing director
- The registered office of the company is at the address of a domicile/office service provider or at the residence of the managing partner
- The managing director is a citizen of a neighbouring country to the east and does not yet have a longer history in Austria (residence only recently registered or not yet or only recently recorded for tax purposes). In general, a registered place of residence in Austria should not be considered to minimise risk.
- A shell company was used
- After a significant change in ownership, the registered office is relocated (indication of a shell company acquisition)

and the following test steps:

- If it is suspected that a shareholder managing director is a straw man, an income tax assessment could also be requested in order to check whether the company matches the financial capacity of the shareholder managing director. Proof of salary payments could also be requested. If no or unusually low payments are made, this could also be an indication of a straw man.

With regard to the threat scenario of **private foundations without reported beneficiaries**, it is recommended to pay attention to the following risk factors:

- The circle of beneficiaries was specified as family members and it can be verified that the founders have (living) descendants
- The foundation deed in the collection of documents of the commercial register contains provisions that suggest the existence of beneficiaries.
- The purpose of the foundation suggests that there are beneficiaries.

and the following test steps:

- Request for copies of the § 5 PSG notifications
- Check whether there are persons who fall into the group of beneficiaries
- Precise analysis of the foundation's purpose in the foundation and foundation charter

With regard to the threat scenario of **circumvention of financial sanctions**, it is recommended to pay attention to the following risk factors:

- In the case of domestic situations, the red flags for the other threat scenarios are also relevant
- Involvement of family members of a sanctioned person or another person close to this person
- Transfers of ownership in a temporal proximity to sanctioning
- Foreign ultimate legal entities in countries with a low level of transparency
- Nominee agreements with foreign ultimate beneficial owners (in particular if the owner is a lawyer, tax advisor, family member or other related party of a sanctioned person).

and the following test steps:

- Request for a historical extract from the Beneficial Owner Register for legal entities suspected of being sanctioned

With regard to the threat scenario of **using associations for the purposes of terrorism financing**, it is recommended to pay attention to the following risk factors:

- The organisational representatives of the association are also the organisational representatives of other similar associations. The risk is increased if there are repeated interruptions over time (= new formation of an association as soon as the previous association becomes conspicuous).
- Citizenship of an organisational representative from a high-risk country or a place of birth in a high-risk country
- Projects in countries listed by the European Commission or the Financial Action Task Force and projects where NPOs have identified terrorist financing risks
- If the organisation has an Austrian Donation Seal of Quality, ADA accreditation and/or ECHO certification, this should be considered risk-reducing (see sectoral risk assessment NPO 2024)

and the following test steps:

- Checking whether the organisation's website matches its purpose
- Carrying out a personal search of the organisational representatives in the Beneficial Owner Register in the event of suspicion
- Check whether other legal entities are registered at the address of the association in case of suspicion

8.2 Foreign legal entities

General description
General information on foreign legal forms: According to the revised FATF Recommendations 24 and 25, as amended in 2022 and 2023, the ML/TF risks of foreign entities to which Austria is exposed should be assessed so that appropriate measures can be taken to counteract the identified risks. As a first step, the FATF recommendations were therefore used to determine which foreign legal entities should be included in the risk assessment due to a significant link: • Branch office in Austria for companies or administration in Austria for trusts, trust-like agreements or foundations • Bank account or a custody account in Austria • Ownership of aircraft • Ownership of ships • Indirect ownership of domestic legal entities due to the position of a ultimate legal entity • Ownership of domestic properties A separate analysis of companies, private foundations and trusts (including trust-like agreements) is only carried out if this is possible due to the data availybility andappears appropriate with regard to the risk situation. When the term legal entity is used in this analysis, it includes companies, private foundations, trusts and trust-like agreements. **Transparency of beneficial ownership:** In certain casesn, information on the beneficial owners of foreign legal entities can only be retrieved from a domestic register. For this reason, the registry authority has published country information for the most important foreign jurisdictions, including China, Jersey, Liechtenstein, Malta, Russia, the United Arab Emirates, the United Kingdom and Cyprus. This country information contains information on the typical legal forms in each country, the documents available for verifying beneficial ownership and the existing registers. In certain cases, however, the beneficial owners can also be retrieved from the Beneficial Owner Register:

- Trusts or trust-like agreements whose administration is not located in Austria or another member state, provided that they enter into a business relationship in Austria or acquired a property after 1 April 2021.
- Companies, foundations and comparable legal entities whose registered office is not located in Austria or another Member State, provided that they undertake to acquire ownership of a property located in Austria.
- Foreign companies, foundations, trusts and trust-like agreements, provided that they are the ultimate legal entity of a domestic legal entity. In this case, in the case of foundations, trusts and trust-like agreements, all beneficial owners are recorded in the register and, in the case of companies, those persons who exercise control over them.

Number of significant affiliations of foreign legal entities by type of significant affiliation:

Type of significant link	Total	Companies	Foundations	Trusts and comparable legal arrangements
Branch office or administration in Austria or business relationship	2.177	2.170	2	5
Bank account or a custody account in Austria	63.232			
Ownership of aircraft	541	538	1	2
Ownership of ships	As the ship register has not yet been digitised, these figures are not available. However, it can be deduced from the sample that the number is rather low. This can also be explained by Austria's geographical location as a landlocked country.			
Indirect ownership of domestic legal entities	9.315	7.878	1.108	329
Ownership of domestic properties	5.099			

Threat

Money laundering

To assess the threat of legal entities being misused for money laundering, two threat scenarios are considered: The use of foreign legal entities, trusts and trust-like agreements for the purpose of concealing beneficial ownership of domestic legal entities and business activities of foreign legal entities, trusts and trust-like agreements for the purpose of financing money laundering.

The threat specific to the legal form is to be derived from available data, assessments by experts from the public and private sectors and publicly available information.

According to the experts, the threat posed by foreign legal entities depends heavily on the respective foreign jurisdiction. The lower the economic connection to Austria, for example if a foreign legal entity only has a domestic bank account, the higher the risk. A distinction must be made as to whether the foreign legal entity itself operates in Austria or whether a foreign legal entity is part of the shareholding structure of a domestic legal entity. For example, regional banks have few foreign legal entities as direct customers, but they do occur in the shareholding structure. Both cases have in common that there are considerable deficits with regard to the transparency of beneficial ownership in the case of foreign legal entities in certain countries. In addition, in some cases there is a lack of knowledge about the various foreign legal entities and their specific characteristics. Knowledge of the foreign legal forms, the available evidence and the possibilities for queries is therefore required in order to determine the beneficial ownership of foreign legal entities.

Depending on the jurisdiction, it can be extremely difficult for obliged entities and authorities to obtain the necessary information. Experts repeatedly cite countries such as Cyprus, Malta, China, the United Arab Emirates, the United Kingdom and all offshore jurisdictions as particularly problematic. In relation to the (Russia) sanctions, legal entities from countries such as Cyprus are also being used to circumvent EU sanctions. Companies, predominantly limited companies, or trusts are used for this purpose. The transparency of Liechtenstein foundations is also problematic, although there are reports of good cooperation in practice. For certain Swiss cantons, the USA, in particular Delaware and Wyoming, and some Dutch companies, there are also frequent problems with identifying beneficial owners and are therefore perceived as high-risk. Austria's neighbouring countries, in particular Hungarian and Eastern European countires, frequently appear in connection with fraudulent activities.

The trust, which originates from the Anglo-American legal system, is considered difficult to define due to its inherent variety of forms. Generally, a trust is when a natural or legal person (the settlor) transfers assets, property or rights (the trust assets) to a second person (the trustee), who manages or utilises the transferred assets in the future for one or more third parties (the beneficiaries) in accordance with the rules established by the settlor with effect against anyone. In the case of trusts, the verification of the origin of the funds and non-transparent structures therefore present difficulties. The

origin of the funds to be laundered often lies in countries such as Russia and Ukraine, but also increasingly in Arab countries. The degree of transparency of trusts varies. In Luxembourg, for example, trusts are well regulated, the structure is usually comprehensible, and they are audited. European countries such as Malta, Cyprus and the Baltic states are considered less transparent.

Ownership of domestic properties by foreign companies and trusts domiciled outside the EEA is often not possible in practice due to restrictions imposed by the property transfer authorities. Therefore, domestic properties are usually acquired by domestic or EEA corporations. Whether land transfer authorities also check the beneficial ownership depends on the respective federal state. The interviews with experts have shown that the property sector is no longer as risky as it used to be, as investments from risky countries are declining and the monitoring of property transactions by credit institutions has intensified. The standards of real estate agents, who have to fulfil their own customer due diligence obligations, have also improved in recent years.

Conclusio:

With regard to the threat of foreign legal entities being misused for money laundering, the opinions of experts do not indicate a generally high threat from foreign legal entities. Nevertheless, threats specific to legal forms were reported. These include, for example, foreign legal entities that are known for their lack of transparency, such as trusts, trust-like agreements and foundations, and are specifically used to conceal beneficial ownership.

There are clear differences in the threat with regard to the type of significant link. While a branch office as a dependent part of a foreign company poses a low threat from the permanent establishment in Austria, the threat is higher in the case of a bank account or a custody account in Austria.
As ships are generally not particularly important in Austria due to its geographical location as a landlocked country, the threat here is classified as 1 - low. However, in the case of aircraft, especially private jets, a higher threat must be assumed, as incriminated assets may have been used for the purchase. Many of the aircrafts are operated by major airlines. These are not considered to pose an increased risk. As only a total of three aircrafts are registered to trusts or a foundation, the threat is assessed across all legal forms, with an overall risk rating of 2 - medium.
Whether the indirect ownership of domestic entities by foreign entities poses a threat depends on the purpose. While an investment in domestic industrial companies is unlikely to be used for money laundering purposes, the threat is higher in the case of domestic entities holding real estate. In such cases, incriminated assets may also have been used for the purchase. Overall, however, a moderate threat can be assumed, which is why risk 2 - medium is assigned. The direct ownership of domestic legal entities by foreign legal entities is also exposed to a lower threat. Due to the strict property transfer regulations and the fact that experts estimate that the risk has decreased, the threat is classified as 2 - medium.

The results of the expert interviews suggest that foreign legal entities within the shareholding structure can significantly impair the transparency of beneficial ownership. This threat depends heavily on the jurisdiction of domicile and the legal form. In particular, legal forms such as foundations and trusts, where obliged entities lack experience, can pose a very high threat to transparency. The risk is further increased if these foundations or trusts are domiciled in jurisdictions that do not cooperate with the respective national authorities across borders and where the lack of transparency is deliberately enabled or at least tolerated. Insofar as a distinction is made between the legal forms, the threat for foreign foundations, trusts and trust-like agreements should therefore be assumed to be one risk level higher than for companies. Otherwise, the overall threat is increased by one level.

Type of significant connection	Companies	Foundations	Trusts and trust-like agreements
Branch office or administration in Austria or business relationship	2 - medium		
Bank account or a custody account in Austria	3 - high	4 - very high	4 - very high
Ownership of aircraft	3 - high		
Ownership of ships	2 - medium		
Indirect ownership by foreign legal entities	2 - medium	3 - high	3 - high
Ownership of domestic properties	3 - high		

Terrorism financing

To assess the threat of the misuse of foreign legal entities for terrorism financing purposes, two threat scenarios are considered: The use of foreign legal entities, trusts and trust-like agreements for the purpose of concealing beneficial ownership and business activities of foreign legal entities, trusts and trust-like agreements that may be used for the purpose of financing terrorism. The legal form-specific threat should be derived from available data, assessments by experts from the public and private sectors and publicly available information.

Terrorists utilise a wide range of both legal and illegal sources of financing. Examples of legal sources of funding include property, stock market investments,wages and salaries. Illegal sources of funding can come from smuggling, fraud, theft, drug trafficking, kidnapping, robbery, arms trafficking and money laundering. Legal and illegal gifts from donors have played a major role in the past. For the transfer of assets, terrorists use the hawala financial system, couriers, money transfer services and cryptocurrencies.
None of the experts interviewed were able to report any concrete experience in connection with terrorism financing by foreign legal entities. It was pointed out that terrorism financing mainly involves a large number of small amounts that are more difficult to detect overall. With regard to terrorism financing, front companies can also be used to channel financial flows along constructed company chains in order to disguise the origin of the funds.

Conclusio:
There were no indications of a high threat from foreign legal entities and trusts with regard to the scenarios relevant to terrorism financing. However, as there is also little experience, the threat was assessed as level 2 - medium to 3 - high. With regard to the lack of transparency, the threat posed by foreign foundations and trusts (as is the case with the threat posed by money laundering) must be rated one risk level higher in each case. Insofar as a distinction is made between the legal forms, the threat for foreign foundations, trusts and trust-like agreements should therefore be assumed to be one risk level higher than for companies. Otherwise, the overall threat is increased by one level.

Type of significant connection	Companies	Foundations	Trusts and trust-like agreements
Branch office or administration in Austria or business relationship	3 - high		
Bank account or a custody account in Austria	3 - high	4 - very high	4 - very high
Ownership of aircraft	3 - high		
Ownership of ships	2 - medium		
Indirect ownership by foreign legal entities	2 - medium	3 - high	3 - high

Ownership of domestic properties	3 - high

Proliferation financing

To assess the threat of misuse of foreign entities for the purpose of proliferation financing, two threat scenarios are considered: The use of foreign legal entities with the aim of concealing beneficial ownership and business activities of foreign legal entities that could be used for proliferation financing. The legal form-specific threat will be derived from available data, assessments by experts from the public and private sectors and publicly available information.

The threat of proliferation financing by foreign legal entities arises above all from the possible concealment of beneficial ownership through complex legal constructs, so that the underlying actors are not disclosed and indirect business relationships are (unknowingly) established with sanctioned jurisdictions. As there are hardly any "significant links" between Austria and the countries at risk for proliferation financing directly due to the sanctions regime, abusive (financial) transactions are carried out via circumvention constructs with neighbouring countries or offshore jurisdictions. No concrete threat scenarios could be reported from practice. However, the high lack of transparency of foreign foundations and trusts poses a particular risk.

Conclusio:

The concealment of beneficial ownership was identified as a relevant threat scenario. As there is little experience, the threat was assessed as level 2 - medium to 3 - high, equivalent to terrorism financing. With regard to the lack of transparency, the threat posed by foreign foundations and trusts (as with the threat posed by money laundering) must be rated one risk level higher in each case. Insofar as a distinction is made between the legal forms, the threat for foreign foundations, trusts and trust-like agreements should therefore be assumed to be one risk level higher than for companies. Otherwise, the overall threat is increased by one level.

Type of significant connection	Companies	Foundations	Trusts and trust-like agreements
Branch office or administration in Austria or business relationship	3 - high		

Bank account or a custody account in Austria	3 - high	4 - very high	4 - very high
Ownership of aircraft	3 - high		
Ownership of ships	2 - medium		
Indirect ownership by foreign legal entities	2 - medium	3 - high	3 - high
Ownership of domestic properties	3 - high		

Vulnerability

Money laundering

In order to assess the weak points in relation to foreign legal entities, the following points are considered:

Share of foreign legal entities

In order to be able to draw conclusions about the share of foreign legal entities in the domestic market, existing branches, bank connections, ownership of aircraft and ships as well as indirect ownership of domestic legal entities due to the position of a supreme legal entity and ownership of domestic real estate are analysed in Austria. The basic assumption behind this is that the risk posed by foreign legal entities increases with their relative share. These figures were set in relation to the number of domestic structures (1 - low: <2%; 2 - medium: 2% to <5%; 3 - high: 5% to <10%; 4 - very high: 10% and above).

There are 2,172 foreign branches registered in the Austrian company register and five foreign trusts registered in the Beneficial Owner Register. A total of 272,347 legal entities are registered in the company register. The proportion of branches is 0.08%.

There are 1,428,672 accounts held by legal entities in Austria. Of these, 63,232 accounts (4.42%) are held by foreign legal entities.

Of the total of 1,312 aircraft registered to legal entities, 786 are registered to domestic legal entities and 541 to foreign legal entities, which corresponds to just under 41%. Vienna International Airport is a major international airport and an important hub for international air traffic. A large proportion of the registered aircraft are large commercial aircraft used by airlines for scheduled services.

A large part of the Austrian ship register was also inspected as part of the data collection process. The data is not available in digitalised form. The index cards were viewed at the main location in the centre of Vienna. Index cards are also stored in other districts, and data on inland waterway vessels is also located in Klagenfurt. In principle, a distinction must be made between seagoing vessels and inland waterway vessels, but this distinction is not relevant for the use of data in the National Risk Assessment. The Austrian shipping register mainly lists natural persons registered in Austria. However, domestic and foreign limited liability companies are also registered. The limited liability companies are based almost exclusively in Austria, Germany, Hungary and Romania. This seems plausible due to the geographical connection to the Danube. Deleted register entries in card form were also randomly checked. No conspicuous pattern emerged. The type and number of notifications relating to foreign and domestic natural persons and legal entities are in a similar ratio. The result of the data collection from the shipping register is therefore that only a low risk of money laundering and terrorism financing by foreign legal entities could be identified from ships registered in the shipping register. It was therefore decided not to inspect other locations in the shipping register. Due to the low relative importance of the sector, risk 1 - low was assigned.

As of 1 January 2025, the scope of application of the WiEReG includes a total of 409,956 legal entities, six of which are domiciled abroad. Indirect ownership of the legal entities is held by 54,977 domestic top-level legal entities (74.43%) and 9,442 foreign top-level legal entities (12.78%). Of these, 7,962 are companies (10.78%), 1,139 are foundations (1.54%), 333 are trusts (0.45%) and 8 are trust-like agreements (0.01%).

There are currently 10.2 million properties in the Austrian land register. Austrian legal entities account for a total of 1,732,551 properties (approximately 17%). Foreign legal entities account for a total of 5,099 properties (approximately 0.04%). The ratio of foreign legal entities to domestic legal entities that own real estate is 0.29%.

Type of significant connection	Risk due to the relative size of the share of foreign legal entities	Data acquisition

Branch office or administration in Austria or business relationship	Low (0.08%), the proportion of trusts and trust-like agreements with a domestic administration or business relationship is even lower, therefore 1 - low overall			Statistical data/Qualitative analysis
Bank account or a custody account in Austria	2 - medium (4.43%)			Statistical data
Ownership of aircraft	4 - very high (40.77%)			Statistical data
Ownership of ships	1 - low			Qualitative analysis
Indirect ownership by foreign legal entities	**Companies** 4 - Very high (10.78%)	**Foundations** 1 - low (1.54%)	**Trusts and trust-like agreements** 1 - low (0.46%)	Statistical data
Ownership of domestic properties	1 - low (0.29%)			Statistical data

Type of business risk

The specific economic activities of legal entities are of great importance for assessing the extent of the vulnerabilities. As no precise information on the specific activities was available in an analysable form, the primary focus was on the type of significant connection, taking into account whether the type of connection also allows conclusions to be drawn about riskier business areas. The assessment was carried out for all groups together.

Type of significant connection	Business activity risk	Reason
Branch office or administration in Austria or business relationship	1 - low	No indications of increased activity in high-risk sectors, therefore a low risk can be assumed

Bank account or a custody account in Austria	2 - medium	Banks are subject to strict supervision by the FMA, which is why only a medium risk can be assumed across all sectors.
Ownership of aircraft	2 -medium	General suitability for money laundering is given, but no national cases are known. The majority of aircraft registered to foreign legal entities are passenger or cargo aircraft belonging to major airlines. This sector does not represent a particular money laundering risk.
Ownership of ships	1 - low	Due to their geographical location, ships do not appear to be suitable for being misused for the purposes of money laundering.
Ownership of foreign legal entities	3 - high	The ÖNACE category "Holding investments" is a risky field of activity. Incriminated assets can also be invested via shareholdings. However, as many legal entities across all Austrian legal entities are also active in non-risky economic sectors, the overall risk is rated as 3 - high
Ownership of domestic properties	3 - high	According to the Money Laundering Report 2023, expensive properties in particular provide a plausible reason for a high use of funds, which is why they are suitable for the purposes of money laundering.

Geographical risk exposure

To determine the geographical risk exposure, the percentage of foreign legal entities domiciled in high-risk countries for money laundering was analysed (1 - low: <2%; 2 - medium: 2% to <5%; 3 - high: 5% to <10%; 4 - very high: 10% and above).

If no statistical data is available, the risk exposure should be determined on the basis of expert opinions.

Type of significant connection	Companies	Foundations	Trusts and trust-like agreements	Data acquisition
Branch office or administration in Austria or business relationship	1 - low (0.60%)	1 - low (0.00%)	1 - low (0.00%)	Statistical data
Bank account or a custody account in Austria	2 - medium (2.42%)			Statistical data
Ownership of aircraft	1 - low (1.66%)			Statistical data
Ownership of ships	1 - low (no complete data set available)			qualitative analysis
Indirect ownership by foreign legal entities	4 - very high (16.97%)	1 - low (0.84%)	1 - low (0.57%)	Statistical data
Ownership of domestic properties	2 - medium (no data available on geographical risk exposure)			-

Transparency of foreign legal entities

For the various types of significant connections of foreign legal entities, the data that can be queried domestically will be analysed. If there are no differences with regard to the various groups, these were summarised for the assessment. It should not be analysed whether this data can be viewed via data sources in the foreign legal entity's country of origin, as this circumstance is already covered by the geographical risk exposure. Both the availability of basic data and information on beneficial ownership were assessed. The transparency of the basic data and the transparency of the beneficial ownership data were each weighted equally, as the basic data can generally also be used to collect the beneficial ownership data.

Type of significant connection	Companies	Foundations	Trusts and trust-like agreements

Branch office or administration in Austria or business relationship	**Basic data:** In accordance with § 3 FBG, all basic data with the exception of founding documents (the associations statutes etc.) are stored (1 - low) **Beneficial ownership:** no domestic data available (4 - very high) **Risk level**: 2.5 - high	**Basic data:** in the case of domestic administration, trusts and trust-like agreements are stored in BOR, which is why all basic data, with the exception of formation documents, is stored Risk level 1 - low **Beneficial ownership:** the data on beneficial owners is stored in BOR. Risk level 1 **Risk level**: 2 - medium (devaluation, as complete coverage cannot be ensured)
Bank account or a custody account in Austria	**Basic data:** In accordance with article 2 KontRegG, the name of the legal entity, the master number of the respective foreign register and the main business address abroad must be reported, but not founding documents. **Beneficial ownership:** The account-holding credit institutions are obliged to collect the beneficial ownership of their customers and report it to the account register. **Risk level:** 1 - low	
Ownership of aircraft	**Basic data:** Pursuant to article 6 of the Civil Aircraft and Aeronautical Equipment Regulation 2010, only the name and address of the aircraft operator must be provided in addition to aviation-specific information. The nationality must only be stated for the aircraft (2 - medium). **Beneficial ownership:** no domestic data available (4 - very high). **Risk level:** 3 - high	
Ownership of ships	**Basic data:** In accordance with the Ship Register Regulations, mainly shipping-specific information is required for the registration of both seagoing vessels (§ 11) and inland waterway vessels (§ 12). In the case of seagoing vessels, the owner, in the case of a shipping company the co-owner and the size of the ship divisions, in the case of a general partnership the partners and in the case of a limited partnership or a partnership limited by shares the personally liable partners must be entered in the shipping register. The legal basis for the acquisition of ownership must also be stated. In the case of inland waterway vessels, the name and address of the owner must be stated; in the case of several owners, the size of the individual shares must be stated. The legal reason for the acquisition of ownership must also be stated. The register is not yet available in digitalised form (1 - low)	

	Beneficial ownership: no domestic data available (4 - very high). **Risk level:** 2 - medium (taking into account the low significance)
Indirect ownership by foreign legal entities	Domestic legal entities in which foreign legal entities hold a stake of more than 25% at the first level and more than 50% at the second level must report these foreign legal entities to the Beneficial Owner Register as ultimate beneficial owners. **Basic data:** Pursuant to article 5 para. 1 no. 2 lit. c, the Beneficial Owner Register contains the basic data of foreign legal entities with the exception of the founding documents (association's statutes, etc.). (1 - low) **Beneficial ownership:** The Beneficial Owner Register contains the data of the beneficial owners of foreign ultimate beneficial owners, provided they exercise control. As not all beneficial owners are stored, the risk is assessed as 2 - medium. **Risk level**: 1.5 - medium
Ownership of domestic properties	**Basic data:** Only the exact details of the property, first name, surname, date of birth and place of residence of the applicant must be entered in the land register for the registration. In the case of legal entities, the name, including the legal form supplement, is stored in the land register. Pursuant to article 5 (1) (2) (c), foreign legal entities that acquire ownership of a domestic property must state the name and registered office of the legal entity, the legal form, the identifiers corresponding to the master number and the master register as well as the proportion of shares, voting rights or the beneficial owner's interest in the ultimate legal entity. (1 - low) **Beneficial ownership:** Data on beneficial ownership is available in the Austrian WiEReG for foreign legal entities subject to reporting requirements. (**1 - low**) **Result:** The basic data is also stored in the land register for those legal entities that are not entered in the Beneficial Owner Register. As all property acquisitions are subject to notarisation, the beneficial owners are also determined and verified by the respective notary and can be requested by the authorities. If the foreign legal entities are entered in the Beneficial Owner Register, the data can be queried online. Overall, **risk level 2 - medium** is therefore assigned, as the ownership of EEA legal entities can only be queried via BORIS and this data is therefore, strictly speaking, not available domestically.

The degree of "attractiveness" for foreign legal entities

According to the OECD, Austria's economy has developed well in recent decades. With its per capita gross domestic product (GDP), the country ranks 9th among the 38 OECD countries. However, high budget deficits have been recorded in recent years as the government cushioned the effects of the coronavirus pandemic and energy price shocks for private households and companies with support measures. By continuing the reforms to increase productivity, improve social mobility and accelerate climate protection, Austria can provide impetus for more growth and further improve living standards, according to a recent OECD study.

The 2016 FATF audit found that Austria has a solid framework for the prevention of money laundering. However, potential for improvement was identified in the areas of national policy coordination, risk assessment and targeted financial sanctions. The FATF follow-up report from 2018 revealed that Austria has made progress in terms of technical compliance since then.

As part of the 2021 National Risk Assessment, Austria has identified increased risks for the Austrian banking sector. These risks include relationships with non-resident customers and politically exposed persons, as well as increasing correspondent banking relationships. The FMA has a comprehensive data basis that allows it to make an informed risk classification. Business relationships with offshore jurisdictions are declining. However, there is room for improvement in the exchange of cross-border data.

While measures to curb money laundering are being strengthened, there is still a risk of money laundering activities involving foreign corrupt funds. According to the 2021 National Risk Assessment, the risk of foreign bribery is medium.

In the Tax Foundation's International Tax Competitiveness Index ranking, Austria is in 15th place overall. Austria is one of the countries that have reduced corporation tax, but only by 2% from 25% to 23%. This puts Austria below the OECD average of 23.9%. Austria offers relatively good cost coverage for machinery and industrial buildings. There are no inheritance, estate or wealth taxes. Weaknesses of the Austrian tax system are the digitalisation tax introduced in 2020 and the high tax and contribution burden on labour, which ranks third among OECD countries. Austria also has a relatively high top tax rate of 55%.

Austria is not a jurisdiction with low tax rates compared to other jurisdictions. There is therefore no tax incentive that makes Austria attractive for foreign legal entities.

The IMF's article IV Consultation considers Austria's current economic situation to be at a pre-pandemic level. Fiscal leeway has been utilised to cushion the impact of the expansion of the Russian war of aggression against Ukraine in 2022.

With regard to money laundering and terrorism financing, the IMF's article IV Consultation points to the increased risks for the Austrian banking sector identified in the 2021 National Risk Assessment. Further efforts are needed, such as removing obstacles to effective investigations and prosecutions, improving measures to prevent and detect foreign bribery and increasing the maximum penalties for companies. In this context, the authorities reported on recent legislative progress, such as the amendment of the Austrian Corporate Criminal Liability Act and the adoption of the Whistleblower Protection Act in 2023. The Austrian Beneficial Ownership Register provides information and guidance in this regard and the Beneficial Ownership Registers Interconnection System (BORIS) will provide access to this information across the EU.

To summarise, it can therefore be stated that Austria's attractiveness for money laundering or terrorism financing can be classified as low.

Terrorism financing

The analysis of the vulnerabilities of foreign legal entities with regard to terrorism financing is generally identical to the previous analysis for money laundering. The following therefore only deals with aspects in which there are differences.

Geographical risk exposure

To determine the geographical risk exposure, the proportion of foreign legal entities domiciled in countries at risk for terrorism financing was analysed

Type of significant connection	Companies	Foundations	Trusts and trust-like agreements	Data basis
Branch office or administration in Austria or business relationship	1 - low (0.23%)			Statistical data
Bank account or a custody account in Austria	1 - low (0.23%)			Statistical data
Ownership of aircraft	1 - low (0%)			Statistical data
Ownership of ships	1 - low (0%)			Qualitative analysis

Indirect ownership by foreign legal entities	1 - low (0.53%)	Statistical data
Ownership of domestic properties	2 - medium (no data available on geographical risk exposure)	-

Proliferation financing

The analysis of the vulnerabilities of foreign legal entities with regard to proliferation financing is generally identical to the previous analysis for money laundering. The following therefore only deals with aspects in which there are differences.

Geographical risk exposure

To determine the geographical risk exposure, the proportion of foreign legal entities domiciled in countries at risk for proliferation financing was analysed.

Type of significant connection	Companies	Foundations	Trusts and trust-like agreements	Data basis
Branch office or administration in Austria or business relationship	1 - low (0.37%)			Statistical data
Bank account or a custody account in Austria	1 - low (0.57%)			Statistical data
Ownership of aircraft	1 - low (0.55%)			Statistical data
Ownership of ships	1 - low (0%)			Qualitative analysis

Indirect ownership by foreign legal entities	1 - low (0.93%)	Statistical data
Ownership of domestic properties	2 - medium (no data available on geographical risk exposure)	-

Risk-minimisation measures

Risk-reducing effects must also be taken into account when assessing the overall risk. It must be taken careto ensure that there is no double counting of effects (to reduce vulnerabilities and to minimise risk). Therefore, the recording of beneficial ownership data in the Beneficial Owner Register was not categorised across the board as risk-reducing. However, the following effects were taken into account:

- Annual obligation to verify beneficial ownership combined with the annual reporting obligation to the register, as this measure leads to a significant increase in the timeliness of the data. (Effect -1)
- Risk-oriented review of beneficial ownership data by domestic credit institutions, as this measure leads to a significant increase in the timeliness of the data. (Effect -0.5)

Type of significant connection	Companies	Foundations	Trusts and trust-like agreements
Branch office or administration in Austria or business relationship	-	-	-1
Bank account or a custody account in Austria	-0,5	-0,5	-0,5

Ownership of aircraft	-	-	-
Ownership of ships	-	-	-
Indirect ownership by foreign legal entities	-1	-1	-1
Ownership of domestic properties	-1	-1	-1

Total risk

Calculation method: 40% threat + 60% vulnerability - risk-reducing measures = total risk.

Money Laundering	Threat			Vulnerability			Inherent Risk			Risk minimisation measures			Total risk		
	Companies	Foundations	Trusts	Companies	Foundations	Trusts	Companies	Foundation	Trusts	Companies	Foundations	Trusts	Companies	Foundations	Trusts
Branch office or administration in Austria or business relationship	2	2	2	1,30	1,30	1,20	1,58	1,58	1,52	0	0	1	1,58	1,58	1,52
Bank account or a custody account in Austria	3	4	4	1,60	1,75	1,60	2,16	2,65	2,56	0,5	0,5	0,5	1,66	2,15	2,06
Ownership of aircraft	3	3	3	2,20	2,00	2,20	2,52	2,4	2,52	0	0	0	2,52	2,40	2,52
Ownership of ships	2	2	2	1,20	1,00	1,20	1,52	1,4	1,52	0	0	0	1,52	1,40	1,52
Indirect ownership by foreign legal entities	2	3	3	2,70	1,50	1,50	2,42	2,1	2,1	1	1	1	1,42	1,10	1,10
Ownership of domestic properties	3	3	3	1,80	1,75	1,80	2,28	2,25	2,28	1	1	1	1,28	1,25	1,28

Financing of terrorism or proliferation	Threat			Vulnerability			Inherent Risk			Risk minimisation measures			Total risk		
	Companies	Foundations	Trusts	Companies	Foundations	Trusts	Companies	Foundation	Trusts	Companies	Foundations	Trusts	Companies	Foundations	Trusts
Branch office or administration in Austria or business relationship	3	3	3	1,30	1,30	1,20	1,98	1,98	1,92	0	0	1	1,98	1,98	1,92
Bank account or a custody account in Austria	3	4	4	1,40	1,50	1,40	2,04	2,5	2,44	0,5	0,5	0,5	1,54	2,00	1,94
Ownership of aircraft	3	3	3	2,20	2,00	2,20	2,52	2,4	2,52	0	0	0	2,52	2,40	2,52
Ownership of ships	2	2	2	1,20	1,00	1,20	1,52	1,4	1,52	0	0	0	1,52	1,40	1,52
Indirect ownership by foreign legal entities	2	3	3	2,10	1,67	1,63	2,06	2,2	2,175	1	1	1	1,06	1,20	1,18
Ownership of domestic properties	3	3	3	1,80	1,75	1,80	2,28	2,25	2,28	1	1	1	1,28	1,25	1,28

Recommendations

Although the analysis of foreign legal entities did not reveal any substantial risks, measures should nevertheless be taken to improve the current regulatory framework:

- A high risk is shown for the ownership of aircraft, which is just above the threshold for a high risk. Nevertheless, risk-mitigating measures should be taken to reduce the risk to a medium level. The analysis also shows that in practice only foreign companies are currently relevant, as only two aircraft are owned by trusts or trust-like agreements. To reduce the risk, it is in any case recommended that companies, foundations and trusts domiciled in a third country that have registered aircraft for non-commercial purposes for a price of at least EUR 7,500,000 in Austria be included in the scope of the Beneficial Owner Register in order to increase the transparency of beneficial ownership and reduce the risk to a medium level (effect -1).
- As it has been shown in practice that obliged entities have difficulties in obtaining information on the legal forms and registers permitted in foreign jurisdictions, country information on the 20 most important jurisdictions should be kept up to date and all types of obliged entities should be proactively informed of this information on a regular basis.
- The connection of obliged entities to the European register network should be promoted at European level. Austria should set a good example with its own connection.
- With regard to foreign legal entities that acquire properties, the low number seems plausible in principle, as EEA companies do not have to be recorded and a domestic legal entity is regularly interposed for the acquisition (this is stored in the BOR and the beneficial owners can be queried there). However, coordination with the foreign legal entities entered in the land register is still recommended.
- The entry of foreign ultimate beneficial owners in the Beneficial Owner Register should be retained even after implementation of the 6th Anti-Money Laundering Directive, as this measure has proven to increase transparency.

9 Financial sector

Sector / Product / Service / Activity
Financial sector/deposits with CIs/FIs
General description
In many cases, credit and financial institutions (CIs/FIs) are the first point of contact for bringing funds into the general financial system. In addition, the widespread distribution and accessibility as well as the relatively low costs make the services of AI/FIs attractive for the use of ML/TF. The Austrian financial sector is traditionally characterised by a high number of AIs, even though the number of AIs is constantly consolidating. Apart from the strong banking penetration of the domestic financial centre, Austrian CIs are also very strongly represented in foreign markets (especially CESEE) due to their strategic location and active participation in European and global financial markets, which is reflected in particular by the number of (foreign) subsidiaries and branches.
Threat
Terrorism financing In the summarised scenarios of the Supranational Risk Assessment (SNRA), the threat of AI/FI assets being misused for terrorist activities was classified as a high to very high risk. Threats exist because terrorists and their supporters use the traditional financial system on the one hand to raise funds to support terrorist activities - both through legal and illegal activities. On the other hand, they also use it to transfer (small) sums of money to areas where terrorist acts are to be carried out. **Conclusion: To summarise, the threat is classified as high.**
Money laundering In the SNRA's summarised scenarios, the threat was classified as a very high risk. Due to the large number of financial products and services offered by AIs/FIs and the processing of payment transactions, there is a particular risk of being misused for money laundering purposes in this context. In particular, transactions in connection with cash, prepaid cards and cash-related financial assets (e.g. time deposits, deposits) with high liquidity lead to an increased risk. Other account types, such as certain types of escrow accounts (see AndKo-SoV) or school savings accounts (see Schulspar-SoV) may be associated with a lower risk. **Conclusion: To summarise, the threat can be classified as high.**
Vulnerability
Terrorism financing In the summarised scenarios of the SNRA, the vulnerability of assets held with CIs/FIs with regard to misuse for the purposes of terrorism financing was classified as high. The national vulnerability is to be derived below. **(a) Risk potential:** The FMA receives data from the Austrian National Bank on all transactions to and from all countries in the world (this data relates to each individual country and covers all incoming and outgoing transactions, both in terms of volume and number). In relation to the total transaction

volume of the Austrian financial market, only a small proportion is carried out in high-risk countries or crisis regions (or neighbouring countries) or originates from such countries. Nevertheless, cross-border transactions harbour increased risks in terms of money laundering, especially if they are linked to high-risk countries or complex transaction chains.

(b) Risk awareness:

With regard to the screening of transactions in/from high-risk countries, AI/FIs use well-calibrated systems in particular in order to counter the risk appropriately.

(c) Legal framework and supervision/governance:

In accordance with article 9a FM-GwG, business relationships and transactions involving high-risk countries result in such customers being classified as high risk and further enhanced customer due diligence requirements must be applied in addition to the due diligence requirements that must be applied in any case. Furthermore, the risk-increasing factors listed in Annex III to article 9 FM-GwG must also be taken into account when categorising a customer.

Conclusion: Based on the summarised scenarios of the SNRA, which suggest a high vulnerability, the framework conditions presented mean that the vulnerability of assets held with CIs/FIs to being misused for the purposes of terrorism financing is to be classified as medium.

Money laundering

In the summarised scenarios of the SNRA, the vulnerability of assets held with CIs/FIs with regard to misuse for money la

undering purposes was classified as high. The national vulnerability is to be derived below.

(a) Risk potential:

The Austrian structure of AI/ FIs is very heterogeneous and serves a large number of different customer and business segments. These range from regionally limited, traditional retail and commercial business to international corporate and investment banking and international private banking. This reflects the general trend for Austrian banks to be active both within the region and across national borders.

(b) Risk awareness:

The Austrian financial market covers a broad spectrum of customers. This includes business relationships with off-shore customers, foreign correspondent banking relationships, business relationships with PEPs, foundations, NPOs and other customer relationships that may harbour an increased risk based on their typology (such as business relationships with customers from regions with an increased geographical risk). As an international banking centre, Austria is also traditionally attractive to foreign customers.

(c) legal framework and supervision/governance:

See above on TF.

Conclusion: Based on the summarised scenarios of the SNRA, which suggest a high vulnerability, the framework conditions set out above mean that the vulnerability of AI/FI assets to being misused for money laundering purposes must be classified as high.

Risk minimisation measures

Due to the size of the AI/FI sector in Austria and its importance for the Austrian financial market as well as the ML/TF risk described above, this sector is the focus of supervision by the FMA. This is reflected in particular in the number of supervisory measures in this area. The type and intensity of these measures is based, among other things, on the specific risk profiles of the CIs/FIs. This ensures a risk-based differentiation between all AIs/FIs when applying supervisory measures.

New developments and methods that emerge in the ML/TF area are presented and discussed by the A-FIU and FMA with the CIs/FIs at joint events. In addition, there is an in-depth exchange of information within the framework of working groups with experts from the business community and the FIU and FMA, among others.
Total risk
In summary, the overall risk for both TF and ML is classified as high.
Recommendations
Further intensified cooperation between the authorities and stakeholders in order to highlight current patterns and trends as well as to take experience into account in the further development of the relevant legal foundations. These measures are aimed at bringing institutions more in line with the expectations of the supervisory authorities, minimising potential risk gaps and promoting a strong compliance culture.

Sector / Product / Service / Activity
Financial sector/proliferation financing - credit, financial and payment institutions
General description
1. Basis and purpose According to UN Security Council Resolution 1540, "proliferation" is defined as the spread of weapons of mass destruction, i.e. nuclear, biological and chemical weapons, and their means of delivery. However, the current FATF recommendations in connection with proliferation relate exclusively to the implementation of UN Security Council resolutions containing targeted sanctions in connection with weapons of mass destruction programmes.[8] Targeted sanctions are usually aimed directly at regime-affiliated natural or legal persons that are considered a threat to international security. The aim is for them to weigh up the political and economic consequences of their behaviour and for states to abandon their proliferation efforts on the basis of this cost-benefit analysis. The targeted UN sanctions against North Korea include embargoes on goods (such as weapons, dual-use goods, raw materials and luxury goods), transport embargoes, travel restrictions and financial measures. Resolution 1718 also established a committee consisting of all 15 members of the Security Council, which is responsible for overseeing the sanctions resolutions against North Korea. This committee reports annually on its activities. At the Austrian level, the Federal Ministry of the Interior/Directorate for State Protection and Intelligence Service is responsible for monitoring compliance with proliferation-related provisions in

[8] In addition to the UN resolutions, bans on proliferation financing also result from EU regulations that are relevant in this area, such as Council Regulation (EU) No. 2018/1542 concerning restrictive measures against the proliferation and use of chemical weapons, Council Regulation (EU) No. 2017/1509 concerning restrictive measures against the Democratic People's Republic of Korea or Council Regulation (EU) No. 267/2012 concerning restrictive measures against Iran.

accordance with the Sanctions Act 2024. The existing resolutions and sanctions measures cover several areas. The Oesterreichische Nationalbank (OeNB), which is tasked with monitoring financial transactions in the area of credit, financial and payment institutions (article 12 para. 2 Sanctions Act 2024), also applies the broad subdivision into terrorism (financing), proliferation and country-specific sanctions measures (e.g. against Russia and Belarus).

Threat

In the summarised scenarios of the Supranational Risk Assessment, the threat was classified as medium to high. The national threat will be derived below.

One of the main proliferation-related threats is the risk of weapons of mass destruction, delivery systems, dual-use goods and related know-how coming into the possession of sanctioned regimes or terrorist organisations or of certain goods being misused for proliferation-relevant purposes contrary to official statements, as well as the associated financing..

Related activities may involve the creation of non-transparent structures and the misuse of legal entities, for example by creating complex corporate structures, acting in a fiduciary capacity or setting up similar non-transparent constructions (off-shore, interposition of non-entrepreneurial companies, etc.), which (wilfully) make it more difficult to verify the identity of the actual beneficial owner or conceal the actual economic content of a transaction.

In the case of transactions with a non-sanctioned person, organisation or entity that is closely affiliated (economically or personally) with a listed person, organisation or entity, it must be considered and examined whether there is an indirect provision of funds and economic resources to sanctioned persons, organisations or entities, which is also prohibited. It is problematic, for example, if fiduciary relationships are not disclosed and are invisible to outsiders, or if (hidden) fiduciary structures are created with the help of intermediary off-shore companies. The examination of such structures or transactions is primarily the responsibility of the account-holding institutions as part of the due diligence and know-your-customer procedures. A high standard of due diligence applies in order to avoid circumvention. The financial sector is most vulnerable to risks arising from weaknesses in systems and controls.

Case studies/new trends:

Sanctioned persons often use complex corporate structures to conceal their potential influence. For example, there are legal entities in which a sanctioned person A holds a 49% stake, which is why the formal criterion of "ownership" would not appear to be fulfilled at first glance. However, it is questionable how the situation should be assessed if, for example, a further 13% are held by a family member of another sanctioned person.

This potential for circumvention is obvious and was also taken into account in the latest amendment to the EU Best Practices[9]. This guide, which is subject to constant review by the Council of the

[9] EU Best Practices Paper 11623/24, para. 63.

European Union, contains non-exhaustive recommendations and identifies key elements for the implementation of EU sanctions. Although the EU Best Practices are non-binding recommendations, they are an authoritative source of practical guidance for both EU economic agents and national competent authorities. Among other things, the Best Practices contain provisions on the interpretation of the terms "ownership" and "control", which are used to determine whether a particular legal entity is controlled by a sanctioned person.

Accordingly, the aggregated ownership of an entity should also be taken into account when assessing ownership structures. For example, if one sanctioned person owns 30% of the entity and another sanctioned person owns 25% of the entity, the entity should generally be considered to be owned by sanctioned persons. Persons who are not themselves sanctioned are not to be directly included in the calculation according to the Best Practices; however, the prohibition of circumvention may make it necessary to include them. This decision is the responsibility of the respective account-holding institution, which is expected to apply sound due diligence.

Furthermore, the European Banking Authority (EBA) has drawn up "Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national sanctions", which will apply from 30 December 2025. These guidelines specify the internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures by financial institutions and payment service providers. These guidelines also include due diligence measures to detect attempts to circumvent restrictive measures.

Conclusion: Overall, the threat can still be classified as medium to high.

Vulnerability

(a) Risk potential:

Determining the actual economic content of transactions and clearly identifying the "beneficial owner" are essential in order to identify and prevent potential violations of sanctions law. It is necessary to implement standardised processes and documentation requirements to prevent sanctions law from being violated or circumvented.

The risk exists in particular in the case of complex, non-transparent corporate structures where ownership and control are difficult to identify. In cross-border situations, the exchange of information, different legal situations or interpretations, foreign deeds and documents, restrictive access to relevant documents, etc. can also make it difficult to verify the ownership and control structure or the economic content of a transaction.

(b) Risk awareness:

Compared to the National Risk Assessment 2021, the OeNB's monitoring and supervisory measures have increased massively (for more details, see Risk mitigation measures, 2.). A high level of risk awareness is also evident among Austrian credit, financial and payment institutions.

The existing monitoring and supervisory measures have shown that Austrian credit, financial and payment institutions have effective strategies, procedures and controls in place to identify sanctioned persons and identify and freeze assets attributable to them.

Credit, financial and payment institutions routinely check all customers during onboarding and on an ongoing basis by comparing databases against UN, EU, UK, US and national sanctions lists. Sanctions lists are updated at least once a day and imported into institutions' systems. Screening is largely automated and generally includes customers, beneficial owners, trustees, authorised representatives, authorised signatories and other related persons. If the screening produces a match, the customer, as a rule, will be flagged and blocked, and the match will be investigated. If the match is confirmed, the accounts assigned to the customer will be frozen, the OeNB will be notified and no transactions to or from these accounts can be carried out. To ensure that the accounts are permanently frozen, the institutions have implemented appropriate internal control steps.

In addition, transactions from credit, financial and payment institutions are compared in real time with the sanctions lists of the UN, the EU, the UK and the US. The screening process is largely automated: sanctions lists are updated at least once a day and imported into the transaction screening system. As soon as an alert is triggered, the transaction is stopped and must be investigated by the responsible members of staff. As long as the transaction is not authorised, it will not be executed. In the event of a confirmed match, the transaction is frozen or returned and reported to the OeNB.

The SNRA also implies a largely functioning sanctions screening (and identifies risks, especially with regard to unlisted (unknown) persons who carry out terrorist activities).

(c) Legal framework and supervision/governance:
The legal framework is primarily contained in the respective legal acts (UN resolutions, EU Regulations). Administrative penal provisions and criminal provisions are laid down in articles 16 et seq. SanktG 2024.

The OeNB is responsible for monitoring compliance with sanctions measures in the area of credit, financial and payment institutions (article 12 para. 2 SanktG 2024). In particular, it exercises its monitoring and information powers pursuant to article 12 para. 3 SanktG 2024. Monitoring and information powers of the OeNB are also provided for in article 5 DevG 2004. Pursuant to article 12 para. 1 SanktG 2024, the Federal Ministry of the Interior must attend to any matters outside the competence of the OeNB.

When monitoring transactions or circumstances with a cross-border element, it is particularly important that the various national competent authorities work together and exchange information.

(d) Human and financial resources:
The OeNB's responsibilities as a public authority in the area of sanctions are carried out by the OeNB's Legal Division. Up to 13 persons are available as needed to fulfil the tasks assigned to the OeNB by article 12 para. 2 SanktG 2024 in the area of credit and financial institutions pursuant to article 1 BWG and the payment institutions named in article 4 no. 4 of the Payment Services Act

2018 - ZaDiG 2018, Federal Law Gazette I No. 17/2018. It should be noted that these persons are also entrusted with other tasks of the Legal Division.

<u>Conclusion</u>: In summary, the vulnerability continues to be classified as medium.

Risk mitigation measures

1. Measures by institutions

As part of their due diligence, institutions must ensure that no funds or economic resources are made available directly or indirectly to any sanctioned person, organisation or entity and that no other transactions prohibited under sanction law are carried out. In addition, reporting and approval requirements must be observed. Credit institutions have implemented IT tools for the internal monitoring of sanctions-related measures. These systems are used to check both transactions and the institution's customer portfolio for matters relevant to sanctions law; transactions can be stopped or accounts frozen on the basis of the check.

When assessing transactions, their underlying purpose and economic substance must be taken into account. The circumstances of the individual case must be considered on a risk-focused basis. For example, determining the beneficial ownership and the actual economic substance of a transaction are relevant in this context. Here too, a risk-based approach to the audit procedures by the respective institution is essential in order to ensure compliance with due diligence. In addition to conducting comprehensive customer due diligence and observing the KYC/KYCC principle, this includes obtaining additional information on the transactions, the origin of the funds used and the purpose and nature of the business relationship. In addition, institutions must ensure more intensive, continuous monitoring of the business relationship and transactions with high-risk customers and update customer documentation on a regular basis. The implementation of suitable processes and measures is not only necessary in order to recognise sanctions-relevant transactions, but also to recognise evasive actions and prevent the execution of the associated transactions. The employees of the institutions are being made aware of this.

Due to the changed threat situation caused by the Russian war of aggression against Ukraine, institutions have significantly improved the strategies, procedures and controls implemented in relation to the implementation of restrictive measures since February 2022. Furthermore, institutions regularly evaluate the effectiveness of the implemented strategies, procedures and controls.

2. Supervisory measures

The OeNB is in regular contact with the sector to be supervised (article 12 para. 2 SanktG 2024), exercises its right to obtain the necessary information and reports by supervised institutions (article 12 para. 3 SanktG 2024) and is also consulted in connection with the assessment of matters that may relate to sanctions. The provision of information and guidelines regarding compliance with sanctions measures is common international practice.

Supervised institutions submit reports to the OeNB on the basis of the applicable legal provisions; information on frozen funds must be emphasised. The OeNB may grant exemptions to the extent permitted by law, for example regarding the release of frozen funds.

As part of on-site inspections in the area of financial sanctions, supervisors evaluate the extent to which the strategies, procedures and controls applied at the inspected credit institution are suitable for ensuring compliance with foreign exchange and sanctions regulations. In addition to the organisational measures (structural and procedural organisation), the IT systems and their use are examined in detail. This includes, in particular, transaction monitoring and the ongoing monitoring of the entire customer base by the inspected institution. The OeNB also conducts individual assessments of transactions and customer relationships with regard to sanctions-relevant issues, including complete and up-to-date documentation on the customer as such, but also on the respective business case. Depending on the business model, the on-site inspection also includes the letter of credit and guarantee business, the bureau de change and precious metal business and cooperation with payment service providers.

In addition, the OeNB has established further supervisory measures in recent years. These include company visits and management meetings. Company visits are one-day on-site measures with a specific focus. The focus is on individual, selected audit topics. As part of a management meeting, the responsible member of the Executive Board of an institution together with the persons responsible for sanctions compliance present how the respective institution is proceeding in the area of sanctions prevention, i.e. strategies, procedures and controls are presented. Finally, a large number of institutions are contacted with management letters, which are standardised requests for information on specific issues.

Due to the changed threat situation caused by the Russian war of aggression against Ukraine, the OeNB's monitoring and supervisory measures have increased massively since February 2022.

3. National and international exchange of information

The OeNB regularly exchanges information with other national and international authorities, ministries and market participants. It is in regular contact with the European Commission and other European authorities in the area of (financial) sanctions via the SIER (Sanctions Information Exchange Repository) platform published and maintained by the European Commission. For example, the OeNB provides the European Commission and other member states with information on the current amounts of frozen assets via SIER on a quarterly basis and submits summarised reports to the European Commission.

In addition, the OeNB exchanges information with other national competent authorities both on an ad hoc case-by-case basis (legal basis is either article 12 para. 6 Sanctions Act 2024 or specific provisions in the EU Regulations) and in regular meetings (e.g. national sanctions task force with members from other national competent authorities and ministries). In matters affecting several EU Member States, there is also a case-by-case exchange between these national competent authorities.

The OeNB regularly takes part in a multilateral exchange, the "Informal Workshop on Sanctions", every six months. This workshop is organised by the competent authority of a member state and

serves as a forum for exchange between the authorities on current topics and cases on an informal basis.

The FMA is the competent authority for AML and CTF supervision in Austria. Based on article 3 para. 4 FM-GwG and article 12 para. 6 SanktG 2024, the FMA and the OeNB exchange information on relevant cases if there is a suspicion of either a violation of financial sanctions or a violation of the FM-GwG.

In some cases, the OeNB is also informed of potentially relevant cases based on findings and data from prudential banking supervision. In these cases, information is exchanged with banking supervisors on a case-by-case basis.

4. Reporting obligations

To make it possible to monitor compliance with financial sanctions by credit, financial and payment institutions, credit, financial and payment institutions are subject to certain reporting obligations (ad hoc, quarterly and annual reports). The reporting obligations arise either directly from the respective legal act (UN resolution, EU Regulation) or from the Sanctions Act 2024 and are manifold. The OeNB therefore provides numerous reporting templates on its website. These templates contain both definitions and precise descriptions of the data to be submitted to the OeNB. For example, the OeNB collects and validates reporting templates for certain deposits and frozen funds and economic resources.

In the event of violations of reporting obligations, the respective institution subject to the reporting obligation is subject to an administrative fine by the competent federal administrative authority in accordance with article 18 (2) SanktG 2024.

5. Guidance

The OeNB is regularly contacted by market participants (e.g. credit institutions, companies, private individuals) regarding the interpretation of individual provisions or with other enquiries. The OeNB is not legally obliged to provide general legal advice. However, the OeNB is committed to providing certain guidance and orientation to market participants. On the one hand, enquiries are answered thoroughly and quickly in order to provide market participants with the best possible support. In addition, the OeNB regularly publishes questions and answers of general relevance in a guide that is available on its website. The 19th version of this guide has already been published. The OeNB is also in regular contact with the Austrian Federal Economic Chamber (banking association), which can pass on relevant information and changes to obligations or designations to market participants in a targeted manner.

Total risk

Due to the changed threat situation caused by the Russian war of aggression against Ukraine, the OeNB's monitoring and supervisory measures have increased massively since February 2022 compared to the 2021 National Risk Assessment. This shows that Austrian credit, financial and payment institutions have significantly improved their strategies, procedures and controls and adapted them to the new challenges. As a result, they are able to recognise potential circumvention

structures at an early stage and mitigate risks. The financial sector is also generally recognised by the FATF as having a good understanding of the dangers and risks in the relevant compliance areas[10] **To summarise, the overall risk is classified as medium**.
Recommendations
In view of the discussed challenges that may arise in relation to cross-border transactions and circumvention structures, it seems absolutely necessary to enhance the (cross-border) exchange between authorities.

Sector / Product / Service / Activity
Financial sector/investment companies (KAG) - Real estate investment companies (Immo-KAG) - Alternative investment fund managers (AIFM)
General description
KAGs under the InvFG 2011 and Immo-KAGs under the ImmoInvFG formally fall under the term credit institution in Austria, as the management of investment funds and real estate funds under the InvFG/ImmoInvFG is standardised as banking business under the BWG. A KAG or ImmoKAG is a credit institution pursuant to the BWG that is authorised to administer and manage (real estate) assets in accordance with strict Directives. In addition, the AIFMG provides for the licensing and registration of AIF managers. Both KAG/Immo-KAG and - licensed and registered - AIFM are obliged entities under the FM-GwG and must fully comply with the due diligence and reporting requirements for the prevention of ML/TF. Clients of KAG/Immo-KAG require a custodian organisation, which must be a licensed credit institution. In particular, the origin of the funds to be invested is therefore already verified or fulfilled by the custodian CI in a first step.
Threat
Terrorism financing In the SNRA's summarised scenarios, the threat of KAG, Immo-KAG and AIFM being misused for terrorist activities was classified as a low risk. Based on the current information and data available, there are no concrete indications of a threat situation in Austria either. **Conclusion: To summarise, the threat can be classified as low.**
Money laundering In the SNRA's summarised scenarios, the threat was classified as high risk. In the case of investments in investment funds, real estate funds and alternative investment funds, there may be a risk of abuse for money laundering purposes, particularly in connection with well-trained persons (groups) who deliberately misuse such investments and the necessary transactions to conceal the original origin of the funds. **Conclusion: To summarise, the threat can be classified as medium.**
Vulnerability

[10] FATF, MER (2016), 226.

Terrorism financing

In the summarised scenarios of the SNRA, the vulnerability of KAG, Immo-KAG and AIFM with regard to abuse for the purposes of terrorism financing was classified as low. The national vulnerability is to be derived below.

The supervisory practice of the FMA and the available data and information show that services and products in the area of KAG/Immo-KAG and AIFM do not currently lead to any particular vulnerability of the Austrian financial market to being misused for terrorism financing purposes.

Conclusion: Based on the summarised scenarios of the SNRA, which suggest a low vulnerability, the framework conditions presented mean that the vulnerability of KAG, Immo-KAG and AIFM to being misused for the purposes of terrorism financing can be classified as low.

Money laundering

In the SNRA's summarised scenarios, the vulnerability of KAG, Immo-KAG and AIFM with regard to abuse for the purposes of money laundering was classified as medium to high. The national vulnerability is to be derived below.

(a) Risk potential:

The risk classification data indicates moderate geographical risks in connection with the residence of customers in countries with increased risks.

However, the supervisory practice of the FMA and show that services and products in the area of KAG/Immo-KAG and AIFM do not lead to any particular vulnerability of the Austrian financial market to being misused for money laundering purposes beyond the threat situation described above.

(b) Risk awareness:

Over 40% of the supervised entities in this sector have established processes to ensure that ML/TF issues are regularly reported to the supervisory board in writing. In addition, information is available that 94% of the supervised institutions in this sector also regularly train employees outside the area of ML/TF prevention through targeted training programmes on these topics.

(c) legal framework and supervision/governance:

KAG/Immo-KAG and - licensed and registered - AIFM are obliged entities under the FM-GwG and are subject to supervision by the FMA in this regard. The KYC profile of a client plays a key role in the provision of services by KAG/Immo-KAG and AIFM. Although unusual transactions or activities may also follow certain typologies in this area, it is important, particularly in the case of services provided by KAG/Immo-KAG and AIFM, that the obliged entities have sufficient knowledge of their clients and their investment profile. In addition to the investment behaviour of the customer, the subsequent disposal (e.g. payout) of the invested assets must also be taken into account.

Conclusion: Based on the summarised scenarios of the SNRA, which suggest a medium to high vulnerability, the framework conditions presented mean that the vulnerability of KAG, Immo-KAG and AIFM to being misused for the purposes of money laundering can be classified as medium.

Risk minimisation measures

As obliged entities under the FM-GwG, KAG/Immo-KAG and AIFM are covered by the supervisory measures of the FMA. The FMA carries out supervisory measures to prevent ML/TF directly at the obliged entities mentioned, as well as at the custodian banks and depositary banks.
Total risk
In summary, the risk for TF is classified as low and for ML as medium.
Recommendations
Further intensified cooperation between the authorities and stakeholders in order to highlight current patterns and trends and to take experience into account in the further development of the relevant legal bases. Thematic supervisory measures to review the effectiveness of the application of (enhanced) due diligence and reporting obligations by obliged entities in this sector.

Sector / Product / Service / Activity
Financial sector/investment firms and investment services providers
General description
In addition to credit institutions, investment firms and investment services providers that are authorised to provide investment services on a commercial basis in accordance with the WAG 2018 are also relevant in the provision of investment services. Many investment service providers use external intermediaries in the provision of investment services and in sales, who act as agents (contractually bound intermediaries or securities intermediaries) for the investment service provider.
Threat
Terrorism financing In the summarised scenarios of the SNRA, the threat of investment firms or investment services providers being misused for terrorist activities was classified as low risk. Based on the current information and data available, there are no concrete indications of a threat situation in Austria either. **Conclusion: To summarise, the threat can be classified as low.**
Money laundering In the SNRA's summarised scenarios, the threat was classified as high risk. A large number of conduct of business rules - independent of the provisions of the FM-GwG - must be complied with in advance when providing investment services in accordance with the WAG 2018, which means that a comprehensive customer profile is already created. However, as clients such as private foundations, clients from third countries, etc., are also serviced, there is a corresponding residual risk here, which is confirmed by the risk classification data and shows moderate geographical risks in connection with the residence of clients in countries with increased risks. **Conclusion: To summarise, the threat can be classified as medium.**
Vulnerability
Terrorism financing

In the summarised scenarios of the SNRA, the vulnerability of investment firms and investment services providers with regard to abuse for the purposes of terrorism financing was classified as low. The national vulnerability is to be derived below.

The available data and information show that services and products in the area of investment services do not currently lead to any particular vulnerability of the Austrian financial market to being misused for terrorism financing purposes.

Conclusion: Based on the summarised scenarios of the SNRA, which suggest a low vulnerability, the framework conditions presented mean that the vulnerability of investment firms and investment services providers to being misused for the purposes of terrorism financing can be classified as low.

Money laundering

In the summarised scenarios of the SNRA, the vulnerability of investment firms and investment services providers with regard to misuse for money laundering purposes was classified as high. The national vulnerability is to be derived below.

(a) Risk potential:

Both the investor profile and the KYC profile of a client play a key role in the provision of investment services. Unusual transactions or activities can follow certain typologies in this area.

(b) Risk awareness:

Due to the different (personal) circumstances of each investor, it is important that investment service providers have sufficient knowledge of their clients, their financial circumstances and their investment profile in order to be able to recognise any deviations from the expected behaviour or transactions without any recognisable economic benefit. In addition to the customer's investment behaviour, the focus will in any case be on the subsequent disposal (e.g. payout) of the invested assets. In this context, investments with a short investment horizon and a lack of awareness of the costs incurred are subject to increased risk.

(c) legal framework and supervision/governance:

In accordance with the provisions of the WAG 2018, extensive information about the customer must be obtained. Irrespective of this, investment firms and investment services providers must also comply with the provisions of the FM-GwG and carry out a corresponding risk-based review. Only once this comprehensive analysis has been carried out does the actual transaction take place, whereby the investor's custodian and/or account-holding bank must also carry out its own additional review.

Conclusion: Based on the summarised scenarios of the SNRA, which suggest a high vulnerability, the framework conditions presented mean that the vulnerability of investment firms and investment services providers to being misused for the purposes of money laundering must be classified as medium.

Risk minimisation measures

Due to the size of the investment services sector in Austria and its importance for the Austrian financial market as well as the ML/TF risk described above, this sector is also the target of supervisory measures by the FMA. This is reflected in particular by corresponding supervisory measures and the intensification of the exchange of information and experience in this area.

Total risk

In summary, the risk for TF is classified as low and for ML as medium.

Recommendations

Further intensified cooperation between the authorities and stakeholders in order to highlight current patterns and trends and to take experience into account in the further development of the relevant legal bases. Thematic supervisory measures to review the effectiveness of the application of (enhanced) due diligence and reporting obligations by obliged entities in this sector.

Sector / Product / Service / Activity
Financial Sector/Private Banking-Asset *Management*
General description
Private banking primarily serves high-net-worth private clients who invest assets. Such services often include the offering of complex products, the execution of high-volume transactions and a high degree of discretion/confidentiality with regard to the business relationship.
Threat
Terrorism financing Based on the information and data currently available, there are no concrete indications of a threat situation. **Conclusion: To summarise, the threat can be classified as low.**
Money laundering In the SNRA's summarised scenarios, the threat was classified as a high to very high risk. *Private banking client segments* can be characterised in particular by the following features: a high transaction and/or investment volume; the use of complex products and services; the use of legal entities with complex, opaque ownership and control structures (possibly with links to offshore territories - in many cases for tax optimisation reasons) and the client's expectation of increased confidentiality and discretion. *Private banking* services and products are also exposed to an increased risk of being misused for money laundering against the background of the risk factors "client" and "geographical areas". The target group is wealthy private customers with a relatively high proportion of politically exposed persons, including foreigners, compared to the traditional retail business. The use of complex, cascading corporate structures, which often have links to offshore territories, makes it even more difficult to fully trace the origin of the funds used and the actual beneficial owners of these legal entities. **Conclusion: To summarise, the threat is classified as high.**
Vulnerability
Terrorism financing The supervisory practice of the FMA and the available data and information show that services and products in the area of *private banking* do not currently lead to any particular vulnerability of the Austrian financial market to being misused for terrorism financing purposes. **Conclusion: Based on the summarised scenarios of the SNRA, which do not suggest any vulnerability, the framework conditions presented mean that the vulnerability of services and products in the area of *private banking* to being misused for the purposes of terrorism financing can be classified as low.**
Money laundering

In the SNRA's summarised scenarios, the vulnerability of *private banking* services and products with regard to misuse for money laundering purposes was classified as high to very high. The national vulnerability is to be derived below.

(a) Risk potential:

In relation to the entire Austrian financial market, the *private banking* sector represents a relatively small share.

(b) Risk awareness:

With regard to the *private banking* sub-risk, 28.7% of the obliged entities are in the low risk class, 24.2% in the medium risk class, 44.1% in the increased risk class and 3% in the high risk class.

(c) legal framework and supervision/governance:

Private asset management and *private banking* represent risk-increasing factors in accordance with Annex III to article 9 FM-GwG. Obliged entities that offer services and products in the area of *private banking* must take this into account at the level of both their company and customer risk analysis and must take appropriate risk-reducing measures. This includes, for example, additional information and in-depth documents on the beneficial ownership of the customer, the origin of the funds used and the purpose and nature of the business relationship (this may be particularly relevant, for example, in the case of customers from offshore territories who have no other links to Austria and/or do not engage in any operational activities). In addition, institutions must ensure more intensive continuous monitoring of the business relationship (and transactions) with such clients and shorten the intervals for updating the documents/information obtained.

<u>Conclusion</u>: Based on the summarised scenarios of the SNRA, which suggest a high to very high vulnerability, the framework conditions presented mean that the vulnerability of services and products in the *private banking* sector to being misused for money laundering purposes can be classified as medium to high.

Risk minimisation measures

A high number of private banking clients in relation to the total client base represents a risk-increasing factor in the context of risk classification. Classification in a higher risk category results in more intensive monitoring by the FMA, which also shortens the interval between supervisory measures by the FMA accordingly, up to annual supervisory measures. The FMA has carried out and continues to carry out special supervisory measures focussing on the *private banking* customer segment at the obliged entities concerned. In this context, compliance with the customer due diligence requirements to determine the identity of the customer's beneficial owners and to obtain and verify information on the origin of the funds used is a particular focus.

Total risk

In summary, the risk for TF is classified as low and for ML as medium to high.

Recommendations

Further intensified cooperation between the authorities and stakeholders in order to highlight current patterns and trends and to take experience into account in the further development of the relevant legal bases.

Sector / Product / Service / Activity
Financial sector/crowdfunding

General description
For the regulatory assessment of alternative forms of corporate financing and investment, it is important how the form of financing is organised in detail. With the entry into force of Regulation (EU) 2020/1503 on European Crowdfunding Service Providers (ECSP Regulation) on 10 November 2021, a European regime for the provision of crowdfunding services was created, for the enforcement of which the FMA was entrusted with the authorisation and supervision of crowdfunding service providers as the competent authority as of 31 December 2021. Providers under the AltFG are not supervised by the FMA. The BVBs are responsible for enforcing the AltFG. In terms of supervisory law, the supervisory authorities focus on those forms of crowdlending or crowdinvesting in which investors receive financial consideration in the form of money (interest, capital, profit sharing) for their investment. If the consideration for the investor is in material form (e.g. initial access to new products and services) or in symbolic form (such as a personal letter of thanks), this is not considered a capital investment. Donation- or reward-based crowdfunding is generally only affected by Austrian financial market supervisory laws where the platform also handles payment processing between the investors and the projects. In this case, a licence may be required in accordance with ZaDiG 2018. In contrast, when operating a crowdinvesting platform, the licence requirement depends on the type of investment on the one hand and the type of platform activity on the other (e.g. credit brokerage platforms or if the investment is structured as a deposit business [licence under the Austrian Banking Act]; platforms that broker transferable securities or other financial instruments or provide personal investment recommendations [licence under the Austrian Securities Supervision Act 2018 and authorisation under the European Crowdfunding Regulation - ECSP Regulation]). In the case of projects in which the receiving company invests in other companies and is not itself operationally active, the Alternative Investment Fund Manager Act (AIFMG) may regularly apply. If a crowdfunding project or the operation of a crowdinvesting platform falls under one of the above-mentioned supervisory laws, the provider/operator is generally also an obliged entity under the FM-GwG. With regard to anti-money laundering law, the question of whether crowdfunding service providers (CSPs) within the meaning of the ECSP Regulation are to be regarded as obliged entities has so far remained unanswered. In relation to the provision of crowdfunding services, CSPs have so far been at least indirectly obliged to comply with anti-money laundering law. This results from the mandatory integration of payment service providers (or banks or e-money institutions) in the provision of crowdfunding services. For crowd investments issued under the AltFG, the AltFG contains additional obligations for platforms. If the platform operator is not subject to the provisions of the FM-GwG, it must apply the provisions on the prevention of ML/TF of the Trade Act (GewO) pursuant to articles 365m to 365z (article 5 (2) no. 1 AltFG). This applies in particular to crowdinvesting in the form of investments, for which at least a business licence for commercial investment advice pursuant to article 136a GewO is required (article 5 (1) AltFG). The AltFG also contains obligations for those issuers who do not exclusively use a platform (article 4 (5) AltFG). Supervision in this area is the responsibility of the trade authorities. The ECSP Regulation and the Austrian Swarm Financing Enforcement Act do not currently include any provisions relating to anti-money laundering law. Innovation: According to Regulation (EU) 2024/1624 of 31 May 2024 on the prevention of the use of the financial system

for the purposes of money laundering or terrorist financing, CSPs are included in the scope of application as obliged entities under anti-money laundering law in accordance with the ECSP Regulation (including crowdfunding intermediaries, which are, according to Art. 2 no. 16 lit. a and lit. b Regulation (EU) 2024/1624, among others, more specifically defined companies that are not crowdfunding service providers). This Regulation applies from 10 July 2027.

Threat

Terrorism financing

In the SNRA's summarised scenarios, the threat of crowdfunding being misused for terrorist activities was classified as a medium risk.

The unregulated donation-based crowdfunding sector in particular can be misused for terrorism financing purposes by relatively simple means. Terrorists or their supporters can use these crowdfunding opportunities to raise funds for terrorist purposes or to support terrorist activities. Based on the available information and data, such threats may also arise in Austria.

Conclusion: In summary, the threat is classified as medium to high.

Money laundering

In the SNRA's summarised scenarios, the threat was classified as a medium risk. Based on the current information and data available, there are no concrete indications of a threat in Austria that crowdfunding is being misused for money laundering purposes.

Conclusion: To summarise, the threat can be classified as medium.

Vulnerability

Terrorism financing

In the summarised scenarios of the SNRA, the vulnerability of crowdfunding with regard to abuse for the purposes of terrorism financing was classified as medium. The national vulnerability will be derived below.

(a) Risk potential:

In Austria, there is a broad network of regulatory provisions that could apply in connection with crowdfunding projects or platforms. In these cases, the operator is supervised by the FMA in the area of financial market supervision laws with regard to the prevention of ML/TF. If the AltFG applies, the trade authorities are responsible for this.

(b) Risk awareness:

In those cases that do not fall under any of the above-mentioned supervisory laws, a supervised financial market intermediary is required in most cases for the onward transfer of the collected funds. As obliged entities subject to customer due diligence to prevent ML/TF, they must pay very close attention to the origin of the funds, especially when depositing large amounts of cash or receiving many small amounts within a short period of time that quickly add up to a large total sum.

(c) legal framework and supervision/governance:

Operators of crowdfunding projects or platforms must, if they are obliged entities under the FM-GwG, apply the applicable due diligence and reporting obligations in full – or in accordance with the provisions of the AltFG only the articles 365m to 365z Trade Act 1994 if the AltFG is applicable. As obliged entities under the FM-GwG, AIs/FIs must obtain additional information and proof of the origin of the funds, in particular in the case of (cash) deposits of higher amounts (this represents a risk-increasing factor in any case). This is also an important risk-minimising measure, especially for those areas in which crowdfunding projects or platforms are not subject to

regulation and in which funds are to be collected for terrorist purposes by collecting smaller amounts.

Conclusion: Based on the summarised scenarios of the SNRA, which suggest a medium vulnerability, the framework conditions presented mean that the vulnerability of crowdfunding to being misused for the purposes of terrorism financing can be classified as medium to high.

Money laundering

In the SNRA's summarised scenarios, the vulnerability of crowdfunding with regard to abuse for the purposes of money laundering was classified as medium. The national vulnerability will be derived below.

The supervisory practice of the FMA and the available data and information do not indicate any further vulnerability of the Austrian financial market (currently only two crowdfunding service providers are active in Austria).

Conclusion: Based on the summarised scenarios of the SNRA, which suggest a medium vulnerability, the framework conditions presented mean that the vulnerability of crowdfunding to being misused for money laundering purposes can be classified as medium.

Risk minimisation measures

The operators of crowdfunding projects or platforms covered by the financial market supervisory laws are supervised by the FMA as obliged entities under the FM-GwG with regard to compliance with the customer due diligence requirements for the prevention of ML/TF. In addition, the competent trade authorities monitor compliance with the relevant obligations under the AltFG or the GewO in those cases in which the AltFG applies.

Total risk

In summary, the risk for TF is classified as medium and for ML as medium.

Recommendations

Further intensified cooperation between the authorities and stakeholders in order to highlight current patterns and trends and to take experience into account in the further development of the relevant legal bases.

Sector / Product / Service / Activity
Financial sector/bureaux de change
General description
Bureaux de change can be used in particular to change (incriminated) funds into higher-denomination banknotes. This process can be a first step in the context of cross-border cash transfers. No major preparations or planning are required to carry out a currency exchange and it can therefore be carried out relatively easily.
Threat

Terrorism financing

In the SNRA's summarised scenarios, the threat of bureaux de change being misused for terrorist activities was classified as a high risk.

Especially in areas close to borders and at airports, terrorists and their supporters can use bureaux de change to transport cash to crisis regions after changing it into higher-denomination

banknotes to support terrorist groups and activities. However, there is only an increased risk in this context if bureaux de change are located in an area close to the border with crisis regions.
Conclusion: In summary, the threat is classified as medium to high.

Money laundering

In the SNRA's summarised scenarios, the threat was classified as high risk.
Exchange offices can be misused to change incriminated (foreign) funds into - possibly higher denominated - euro amounts.
Conclusion: In summary, the threat is classified as medium to high.

Vulnerability

Terrorism financing

In the summarised scenarios of the SNRA, the vulnerability of bureaux de change with regard to abuse for the purposes of terrorism financing was classified as high. The national vulnerability is to be derived below.

(a) Risk potential:

Due to Austria's geographical location, there is little incentive to change foreign money (foreign currency) into higher-denomination euro money via exchange offices in Austria. The possible transport routes for use for terrorist purposes in crisis areas would be long and therefore offer little incentive for terrorists or their supporters. However, foreign money (foreign currency) can be exchanged into euro amounts via bureaux de change, which are then used to finance terrorist activities in Austria.

(b) Risk awareness:

The ongoing trend towards cashless payments reduces the risk of bureaux de change being misused for ML/TF purposes. Furthermore
Bureaux de change are predominantly offered by fully licensed banks, as a licence is required to operate this business model.

(c) legal framework and supervision/governance:

As obliged entities under the FM-GwG, bureaux de change must apply the relevant due diligence and reporting obligations in full.
Conclusion: Based on the summarised scenarios of the SNRA, which suggest a high vulnerability, the framework conditions presented mean that the vulnerability of bureaux de change to being misused for the purposes of terrorism financing can be classified as medium to high.

Money laundering

In the SNRA's summarised scenarios, the vulnerability of bureaux de change with regard to misuse for money laundering purposes was classified as high. The national vulnerability is to be derived below.

(a) Risk potential:

In order to channel incriminated funds that have been exchanged into euro amounts via an exchange office into the financial system, they must be deposited with an obliged entity under the FMLA (see above under *"Financial sector/deposits with credit and financial institutions"*).

(b) Risk awareness:

See above on TF.

(c) legal framework and supervision/governance:

Higher amounts of money in particular represent a risk factor for increased risk when depositing and in such cases the origin of the funds must be examined particularly closely. One risk-reducing factor is the fact that exchange offices in Austria require a licence from the FMA as a CI and are therefore fully obliged to comply with the due diligence and reporting obligations of the FM-GwG.
Conclusion: Based on the summarised scenarios of the SNRA, which suggest a high vulnerability, the framework conditions presented mean that the vulnerability of bureaux de change to being misused for the purposes of money laundering is to be classified as medium to high.

Risk minimisation measures

As CIs, bureaux de change are obliged entities under the FM-GwG and are therefore covered by the supervisory measures of the FMA.

Total risk

In summary, the risk for both TF and ML can be categorised as medium to high.

Recommendations

Further intensified cooperation between the authorities and stakeholders in order to highlight current patterns and trends and to take experience into account in the further development of the relevant legal bases.

Sector / Product / Service / Activity
Financial sector/electronic money (e-money)
General description
Only e-money issuers are authorised to issue e-money. These include AI and e-money institutions (FMA licence). E-money systems can also exist as regional value unit systems and cards for branch networks or groups of companies. If these systems are so-called "limited" networks, the issuer is not obliged to obtain a licence from the FMA (but is subject to an exemption provision).
Threat
Terrorism financing In the SNRA's summarised scenarios, the threat of e-money being misused for terrorist activities was classified as a high risk. For terrorists or their supporters, e-money products can offer advantages over cash, especially if certain activities are to be carried out online (e.g. hotel bookings or car hire reservations). An additional risk-reducing factor is the traceability of payments with e-money products. **Conclusion: In summary, the threat is classified as medium to high.**
Money laundering In the SNRA's summarised scenarios, the threat was classified as high risk. In most cases, e-money products can only be loaded with certain (sometimes relatively low) amounts, as the issuers of such products stipulate certain amount limits of their own accord. **Conclusion: To summarise, the threat can be classified as medium.**
Vulnerability
Terrorism financing In the summarised scenarios of the SNRA, the vulnerability of e-money with regard to misuse for the purposes of terrorism financing was classified as high. The national vulnerability is to be derived below. **(a) Risk potential:**

Although only a small number of e-money issuers operate in Austria under the freedom of establishment, 245 e-money issuers from other member states are authorised to offer their products in Austria under the freedom to provide services. The latter are not supervised by the FMA with regard to the prevention of ML/TF, but by the respective competent supervisory authority in the home Member State.

(b) Risk awareness:

AML colleges for e-money issuers operating within the framework of a branch in Austria have been established and an official exchange of information and risks takes place in this way.

(c) legal framework and supervision/governance:

As obliged entities under the FM-GwG, e-money issuers must apply the relevant due diligence and reporting obligations in full and are supervised by the FMA.

Conclusion: Based on the summarised scenarios of the SNRA, which suggest a high vulnerability, the framework conditions presented mean that the vulnerability of e-money to being misused for the purposes of terrorism financing can be classified as medium.

Money laundering

In the SNRA's summarised scenarios, the vulnerability of e-money with regard to misuse for money laundering purposes was classified as high. The national vulnerability is to be derived below.

(a) Risk potential:

See above on TF.

(b) Risk awareness:

See above on TF.

(c) legal framework and supervision/governance:

See above on TF.

Conclusion: Based on the summarised scenarios of the SNRA, which suggest a high vulnerability, the framework conditions presented mean that the vulnerability of e-money to being misused for the purposes of money laundering can be classified as medium.

Risk minimisation measures

As obliged entities under the FM-GwG, e-money issuers are fully covered by the FMA's supervisory measures.

Total risk

In summary, the risk for both TF and ML can be categorised as medium.

Recommendations

Further intensified cooperation between the authorities and stakeholders in order to highlight current patterns and trends and to take experience into account in the further development of the relevant legal bases.

Sector / Product / Service / Activity
Financial sector/payment services
General description
Payment service providers and e-money issuers based in another Member State that perform activities in Austria via service providers, such as agents as defined in article 4 no. 35 ZaDiG 2018, are subject to the scope of application of the FM-GwG with these activities in accordance with

article 23 para. 7 FM-GwG. In order to ensure compliance with the provisions on the prevention of ML/TF and to facilitate supervision by the FMA, these institutions must designate a central contact point to the FMA if they fulfil the requirements of Commission Delegated Regulation (EU) 2018/1108. In the context of the activities of payment service providers, the product of account-unlinked cash transfers should be emphasised in particular.

Threat

Terrorism financing

In the SNRA's summarised scenarios, the threat of payment services being misused for terrorist activities was classified as a high risk.

Terrorists or their supporters may use payment services to transfer funds and to receive/send assets for terrorist activities. In particular, new payment methods can be used (e.g. via mobile phones, prepaid cards or online payments).

Conclusion: To summarise, the threat is classified as high.

Money laundering

In the SNRA's summarised scenarios, the threat was classified as high risk.

Payment services can be misused for money laundering purposes, particularly in the context of the use of money couriers. Criminal organisations use money couriers to transfer incriminated funds to other jurisdictions without disclosing the actual identities of the people acting in the background.

Conclusion: To summarise, the threat is classified as high.

Vulnerability

Terrorism financing

In the summarised scenarios of the SNRA, the vulnerability of payment services with regard to misuse for the purposes of terrorism financing was classified as high. The national vulnerability is to be derived below.

(a) Risk potential:

While payments made through payment service providers are not anonymous, it is relatively easy to carry out cross-border transactions with high-risk customers or high-risk third countries. Other factors include the cash-intensive nature of the services offered, the prevalence of occasional transactions rather than business relationships, the large volume and high speed of transactions.

(b) Risk awareness:

There is therefore an increased risk that Austrian payment service providers will be misused for terrorism financing purposes.

(c) legal framework and supervision/governance:

As obliged entities under the FM-GwG, payment institutions must fully comply with the relevant due diligence and reporting obligations. One of the most important customer due diligence obligations in connection with payment services is the identification of the customer and any existing trustee. In addition, the appropriate training and provision of the necessary (technical) infrastructure to agents is also a key measure.

Conclusion: Based on the summarised scenarios of the SNRA, which suggest a high vulnerability, the framework conditions presented mean that the vulnerability of payment services to being misused for the purposes of terrorism financing can be classified as high.

Money laundering

In the summarised scenarios of the SNRA, the vulnerability of payment services with regard to misuse for money laundering purposes was classified as high. The national vulnerability is to be derived below.

(a) Risk potential:

The information and (transaction) data collected by the FMA do not indicate any particular vulnerability of the Austrian financial market. A risk-increasing factor is the fact that it is not always disclosed and not always recognisable when payment services are used for persons other than the direct customer.

(b) Risk awareness:

See above under (a).

(c) legal framework and supervision/governance:

See above on TF.

Conclusion: Based on the summarised scenarios of the SNRA, which suggest a medium vulnerability, the framework conditions presented mean that the vulnerability of payment services to being misused for the purposes of money laundering must be classified as high.

Risk minimisation measures

The FMA sets thematic priorities as part of its supervisory activities to ensure the application of policies and procedures for the prevention of ML/TF by (foreign) payment institutions, CCPs and agents. As part of the annual risk assessment carried out by the FMA, the business model of each payment institution is evaluated. This ensures that payment institutions with a higher risk are subject to increased supervisory intensity. In addition, high standards are set as part of the notification process and it is checked how the notifying company will fulfil the legal requirements of the FM-GwG.

Total risk

In summary, the risk for both TF and ML can be classified as high.

Recommendations

Further intensified cooperation between the authorities, including within the framework of the AML colleges, and stakeholders in order to highlight current patterns and trends as well as to take experience into account in the further development of the relevant legal bases.

Sector / Product / Service / Activity
Financial sector/virtual currencies
General description
Virtual currencies or transactions with virtual currencies (or crypto assets) have limited transparency. This is due to the following risk factors, among others: distributed ledger technology (DLT) used or DLT-like technology or protocols (e.g. DeFi, DApps, etc.); type and mode of operation of the virtual currency or crypto asset (e.g. anonymity-enhanced cryptocurrencies, non-fungible cryptocurrencies, non-fungible cryptocurrencies). of the crypto asset (e.g. anonymity-enhanced cryptocurrencies, non-fungible tokens [NFTs], etc.); technology-based

methods of obfuscation (mixers, tumblers, etc.); distribution channel (e.g. crypto ATMs, prepaid cards; use in connection with Hawala, etc.); products and services (e.g. lending, staking, etc.) as well as (different) regulatory standards and location of the parties involved. This "semi-transparency" should also be seen in conjunction with the possibility of using so-called self-hosted wallets, which provides another option for anonymous transactions.
The limited transparency, a certain degree of "pseudonymity" as well as the fast and cross-border processing of transactions with virtual currencies (crypto assets) thus entail a high risk of virtual currencies (crypto assets) being misused for the purposes of money laundering and terrorism financing.

Based on the new harmonised legal bases, Regulation (EU) 2023/1114 (MICAR) and Regulation (EU) 2023/1113 ("Travel Rule") as well as the AML package, the aim is to combat the risk of money laundering and terrorism financing with the aim of harmonised European supervision of service providers in relation to virtual currencies (providers of crypto-asset services). Although the new European legal framework makes a significant contribution to minimising risk in this area, the rapid technological and business model-specific developments in the area of virtual currencies (crypto assets) mean that appropriate monitoring systems still need to be implemented, know-how built up and, in particular, the "gatekeeper function" to the traditional financial sector adequately included in the measures to minimise the risk of money laundering and terrorism financing.
Especially since insufficient know-how, inadequate monitoring systems and controls, etc. can significantly increase the risk of misuse for money laundering and terrorism financing purposes, not only for service providers in relation to virtual currencies (providers of crypto asset services) but also for traditional financial service providers (AI/FI). Insufficient know-how, inadequate monitoring systems and controls, etc. can significantly increase the risk of misuse for money laundering and terrorism financing purposes, not only for service providers in relation to virtual currencies (providers of crypto asset services), but also for traditional financial service providers (AI/FI).

Threat

Terrorism financing

In the SNRA's summarised scenarios, the threat of virtual currencies (crypto assets) being misused for terrorist activities was classified as a very high risk.
The limited transparency, the increased degree of anonymity when using virtual currencies (crypto assets) and the involvement of the traditional financial system (especially when exchanging virtual currencies - crypto assets for fiat money and vice versa) means that terrorists and terrorist groups are increasingly using them for terrorism financing purposes. As analyses and case studies also show, individual virtual currencies (crypto assets) such as Bitcoin and, in particular, the exchange for fiat money (e.g. exchange for cash via crypto ATMs) in the last phase of terrorism financing (use) are used for terrorism financing purposes.
Conclusion: To summarise, the threat can be classified as very high.

Money laundering

In the SNRA's summarised scenarios, the threat of virtual currencies (crypto assets) being misused for money laundering was classified as a very high risk.

The limited transparency, the increased degree of anonymity when using virtual currencies (crypto assets) and the involvement of the traditional financial system also pose an increased risk in the area of money laundering.

In particular, the use of cash when buying or selling virtual currencies (crypto assets), their use as a means of exchange or payment on the darknet (e.g. via "Bitcoin") and the increased use of stable coins due to their low volatility increase the risk that virtual currencies (crypto assets) will be used to conceal incriminated funds.

Conclusion: To summarise, the threat can be classified as very high.

Vulnerability

Terrorism financing

In the summarised scenarios of the Supranational Risk Assessment, the vulnerability of virtual currencies with regard to misuse for the purposes of terrorism financing was classified as very high. The national vulnerability is to be derived below.

(a) Risk potential:

Based on the information and data available to the FMA, the implementation of strategies, controls and procedures for the prevention of money laundering and terrorism financing by the individual service providers varies depending on the type and complexity of the business model.

(b) Risk awareness:

Based on the information and data available to the FMA, a very different understanding and risk awareness can be recognised among the individual service providers and their different business models.

(c) legal framework and supervision/governance:

As obliged entities under the FM-GwG, service providers in relation to virtual currencies have had to apply the due diligence and reporting requirements of the FM-GwG and the Money Transfers Regulation in full since 10 January 2020. These service providers must register with the FMA before commencing their activities.

Conclusion: Based on the summarised scenarios of the Supranational Risk Assessment, which suggest very high vulnerability, the framework conditions presented mean that the vulnerability of virtual currencies to being misused for the purposes of terrorism financing must be classified as high.

Money laundering

In the summarised scenarios of the Supranational Risk Assessment, the vulnerability of virtual currencies with regard to misuse for money laundering purposes was classified as high to very high. The national vulnerability will be derived below.

(a) Risk potential:

See above on TF.

(b) Risk awareness:

See above on TF.

(c) legal framework and supervision/governance:

See above on TF.

Conclusion: Based on the summarised scenarios of the Supranational Risk Assessment, which suggest a high to very high vulnerability, the framework conditions presented mean that the

vulnerability of virtual currencies to being misused for the purposes of money laundering must be classified as high to very high.

Risk minimisation measures

Since January 2020, virtual currency service providers have been subject to regulation and supervision by the FMA in the area of preventing money laundering and terrorism financing. In the course of supervision, the above-mentioned risk factors became apparent and the ongoing further development of the high supervisory standards led to risk minimisation in the area of ML/TF prevention for service providers in relation to virtual currencies. For example, with regard to a high standard of written strategies, controls and procedures including risk assessment, proof of appropriate expertise and personal reliability of key functions, fit & proper review of the money laundering officer, exchange with other supervisory authorities, etc.).

By repeatedly setting supervisory priorities and consistently pursuing deficiencies, the risk on the Austrian financial market was significantly minimised through revocation proceedings, withdrawals of registrations already made or rejections and withdrawals of registration applications.

With the entry into force of MiCAR at the end of 2024, the high level of supervision in the area of preventing money laundering and terrorism financing will continue in the authorisation procedures and ongoing supervision of new supervised entities in accordance with MiCAR. This is particularly important if new supervised entities (e.g. with international business activities, more complex business models, etc.) enter the Austrian financial centre under the MiCAR regime.

Total risk

In summary, the risk for both TF and ML can be categorised as high to very high.

Recommendations

Further intensified cooperation between national and international authorities in order to draw attention to current patterns, trends and developments as well as to exchange experiences, including from supervisory practice, and to cooperate efficiently in the development of legal bases. The ongoing exchange of experience with stakeholders is also important in order to jointly implement targeted measures to minimise the high risk of money laundering and terrorism financing in this area.

Sector / Product / Service / Activity

Financial sector/life insurance

General description

In addition to the classic function of life insurance (hedging risks), it also has the character of a savings or financial investment and can therefore, like other financial products, be misused for ML/TF purposes. Compared to other financial services, the life insurance business only represents a relatively small share of the Austrian financial market. Some large Austrian insurance groups are also active in foreign markets (especially CESEE).

Threat

Terrorism financing

In the SNRA's summarised scenarios, the threat of life insurance being misused for terrorist activities was classified as a medium risk.

The current information and data situation does not provide any specific indications of a particular threat situation. Above all, the need for very specific expertise makes the use of life insurance for terrorism financing less attractive.

Conclusion: To summarise, the threat can be classified as low.

Money laundering

In the SNRA's summarised scenarios, the threat was classified as a medium risk.

Life insurance policies are open to targeted abuse for money laundering purposes. This is primarily due to the fact that they can be cancelled early and the associated reversal and payout of the amount paid in. However, life insurance policies generally provide for very unfavourable surrender values for the policyholder in the event of early termination. Another risk factor in connection with life insurance policies is the possibility of selling valid life insurance policies on the secondary market (under strict conditions). This has the advantage for the policyholder that the life insurance contract no longer has to be cancelled under unfavourable conditions. Another conspicuous form of life insurance is in combination with loans. Here, existing life insurance policies that were financed with incriminated funds are used to secure loans. After receiving the loan money, the perpetrators then disappear with sufficient legitimisation of the funds. In general, it can be stated that based on the current information and data situation, the threat of life insurance policies being used for money laundering can be categorised as a medium risk.

Conclusion: To summarise, the threat can be classified as medium.

Vulnerability

Terrorism financing

In the summarised scenarios of the SNRA, the vulnerability of life insurance with regard to abuse for the purposes of terrorism financing was classified as low to medium. The national vulnerability is to be derived below.

The supervisory practice of the FMA and the available data and information show that services and products in the area of life insurance do not currently lead to any particular vulnerability of the Austrian financial market to being misused for the purposes of terrorism financing.

Conclusion: Based on the summarised scenarios of the SNRA, which suggest a low to medium vulnerability, the framework conditions presented mean that the vulnerability of life insurance policies to being misused for the purposes of terrorism financing can be classified as low.

Money laundering

In the SNRA's summarised scenarios, the vulnerability of life insurance with regard to misuse for money laundering purposes was classified as low to medium. The national vulnerability is to be derived below.

(a) Risk potential:

Life insurance policies are still popular investment products in Austria. According to generally recognised typologies, single-premium policies (especially in connection with high cash premiums) represent an increased ML/TF risk; however, according to available information, the acceptance of cash in the insurance sector is de facto not relevant in Austria.

(b) Risk awareness:

As the insurance market in Austria is predominantly nationally restricted, the majority of policyholders are natural persons resident in Austria.

(c) legal framework and supervision/governance:

According to the FM-GwG, insurance companies that offer life insurance must fully comply with ML/TF customer due diligence requirements. In addition, the FM-GwG also stipulates that insurance payments may only be made to beneficiaries once they have been identified in accordance with the requirements of the FM-GwG.

Conclusion: Based on the summarised scenarios of the SNRA, which suggest a low to medium vulnerability, the framework conditions presented mean that the vulnerability of life insurance policies to being misused for the purposes of money laundering can be classified as low.

Risk minimisation measures

Due to the relatively small number of insurance undertakings that conduct life insurance business and have to apply the relevant provisions for the prevention of ML/TF, as well as the homogeneity of risk characteristics in the sector due to the restriction to the life insurance sector, the FMA's current supervisory practice ensures comprehensive coverage of the insurance sector.

Total risk

In summary, the risk for both TF and ML can be categorised as low.

Recommendations

Further intensified cooperation between the authorities and stakeholders in order to highlight current patterns and trends and to take experience into account in the further development of the relevant legal bases.

Sector / Product / Service / Activity

Financial Sector/Safe Letting

General description

When providing (renting) safe deposit boxes (safes), the landlord, who is subject to special security obligations, generally provides safe deposit boxes for a fee, typically with a double lock.

Threat

Terrorism financing

Based on the information and data currently available, there are no concrete indications of a threat situation in which the provision of safe deposit box management services is misused by terrorists or terrorist groups for their activities.

Conclusion: To summarise, the threat can be classified as low.

Money laundering

In the summarised scenarios of the SNRA, the threat was classified as high risk. The risk rating is primarily due to the fact that, according to the SRNA, the employees of the safekeeping service are unable to obtain information about the contents of the lockers and that customers have unrestricted access to the facilities.

Safe deposit boxes (safes) can be used to hide incriminated assets in order to subsequently integrate them into the financial system in individual (smaller) tranches. However, it is not possible to convert these assets into non-incriminated assets.

Conclusion: To summarise, the threat can be classified as medium.

Vulnerability

Terrorism financing

The supervisory practice of the FMA and the available data and information show that services and products in the area of safe deposit box management services do not currently lead to any particular vulnerability of the Austrian financial market to being misused for terrorism financing purposes.

Conclusion: Based on the summarised scenarios of the SNRA, which do not suggest any vulnerability, the framework conditions presented mean that the vulnerability of services and products in the area of safe deposit box management services to being misused for the purposes of terrorism financing can be classified as low.

Money laundering

In the SNRA's summarised scenarios, the vulnerability of safe deposit box management services with regard to misuse for money laundering purposes was classified as medium to high. The national vulnerability is to be derived below.

(a) Risk potential:

The majority of safe deposit box management services offered in Austria are the classic form of bank safe deposit box rental by licensed AIs.

(b) Risk awareness:

Safe deposit box management services provided by other companies pose only a low risk; as obliged entities under the FM-GwG, they are also fully subject to the due diligence and reporting requirements of the FM-GwG.

(c) legal framework and supervision/governance:

The provision (rental) of safe deposit boxes (safes) as the provision of safe deposit box management services falls under the business area of FIs within the meaning of article 1 para. 2 BWG. Providers of safe deposit box management services are therefore obliged entities under the FM-GwG and must apply the due diligence and reporting requirements of the FM-GwG in full.

Conclusion: Based on the summarised scenarios of the SNRA, which suggest a medium to high vulnerability, the framework conditions presented mean that the vulnerability of safe deposit box management services to being misused for money laundering purposes can be classified as medium.

Risk minimisation measures

The FMA can impose administrative penalties for violations of the due diligence and reporting obligations under the FM-GwG. The FMA has imposed administrative penalties on providers of safe-deposit box management services who have offered anonymous safe-deposit boxes in the past and thus violated the obligation to identify and verify the identity of their customers.

Total risk

In summary, the risk for TF is classified as low and for ML as medium.

Recommendations

Further intensified cooperation between the authorities and stakeholders in order to highlight current patterns and trends and to take experience into account in the further development of the relevant legal bases.

Sector / Product / Service / Activity
Financial sector/commercial loans
General description

Criminals, terrorists or their supporters use incriminated assets to repay business loans.

Threat

Terrorism financing

In the SNRA's summarised scenarios, the threat of business loans being misused for terrorist activities was classified as a low risk.

Based on the information and data available to the FMA, there are no concrete indications of a threat situation in which terrorist organisations used business loans for terrorism financing.

Conclusion: To summarise, the threat can be classified as low.

Money laundering

In the SNRA's summarised scenarios, the threat was classified as a medium risk.

Based on the information and data available to the FMA, there are no concrete indications of a threat situation in which business loans are used for money laundering.

Conclusion: To summarise, the threat can be classified as medium.

Vulnerability

Terrorism financing

The supervisory practice of the FMA and the available data and information show that services and products in the area of business loans do not currently lead to any particular vulnerability of the Austrian financial market to being misused for terrorism financing purposes.

Conclusion: Based on the summarised scenarios of the SNRA, which suggest a low vulnerability, the framework conditions presented mean that the vulnerability of commercial loans to being misused for the purposes of terrorism financing can be classified as low.

Money laundering

The supervisory practice of the FMA and the available data and information show that services and products in the area of business loans do not currently lead to any particular vulnerability of the Austrian financial market to being misused for money laundering purposes.

Conclusion: Based on the summarised scenarios of the SNRA, which suggest a medium vulnerability, the framework conditions presented mean that the vulnerability of business loans to being misused for money laundering purposes can be classified as low to medium.

Risk minimisation measures

The conclusion of loan agreements is reserved for credit institutions in accordance with article 1 (1) no. 3 BWG and requires a licence from the FMA. In addition to the other customer due diligence requirements of the FM-GwG, AIs must also provide customers with sufficient information regarding the source of funds, for example in the case of loan repayments or repayments that deviate from the original contract. This information must also be verified accordingly by the FI.

Total risk

In summary, the risk for both TF and ML can be categorised as low.

Recommendations

Further intensified cooperation between the authorities and stakeholders in order to highlight current patterns and trends and to take experience into account in the further development of the relevant legal bases.

Sector / Product / Service / Activity
Financial sector/ consumer and small loans
General description
Terrorists and organised crime groups use short-term consumer or small loans with high interest rates but low value. This can be done, for example, by overdrawing the credit card limit with no intention of repaying the overdrawn amount. Consumer or small loans can also be used for money laundering by purchasing expensive goods (e.g. vehicles, jewellery) and repaying them early.
Threat
Terrorism financing In the SNRA's summarised scenarios, the threat of consumer or small loans being misused for terrorist activities was classified as a high risk. Terrorist groups or (radicalised) individuals can use consumer or small loans in particular to finance trips to crisis regions for so-called "foreign terrorist fighters" or for themselves. **Conclusion: In summary, the threat is classified as medium to high.**
Money laundering In the SNRA's summarised scenarios, the threat was classified as a medium risk. Compared to other financial products, consumer or small loans offer little potential to be misused for money laundering - especially to "launder" large amounts of money. **Conclusion: In summary, the threat is classified as medium to high.**
Vulnerability
Terrorism financing In the summarised scenarios of the SNRA, the vulnerability of consumer and small loans regard to abuse for the purposes of terrorism financing was classified as high. The national vulnerability is to be derived below. **(a) Risk potential:** Transaction volumes are generally low and control systems are in place at AIs. The risk may be greater for institutions and intermediaries specialising in fast consumer loans, particularly due to the increased risk of using fake identities, which must also be appropriately assessed when processing a large number of loan applications on a daily basis. **(b) Risk awareness:** Risks can arise in particular where there is little awareness of the setting of transaction monitoring systems or where obliged entities increasingly rely on remote identification options and this is not adequately taken into account by obliged entities. **(c) legal framework and supervision/governance:** In addition to the other customer due diligence requirements of article 6 FM-GwG, AIs must also have sufficient KYC information on the customer. They must also install appropriately configured transaction monitoring systems. **Conclusion: Based on the summarised scenarios of the SNRA, which suggest a high vulnerability, the framework conditions presented mean that the vulnerability of consumer and small loans to being misused for the purposes of terrorism financing can be classified as medium to high.**
Money laundering

In the SNRA's summarised scenarios, the vulnerability of consumer and small loans with regard to misuse for money laundering purposes was classified as medium. The national vulnerability will be derived below.

(a) Risk potential:

Despite the generally low amounts and the relatively low proportion of consumer or small loans, the risk exposure can be high if the obliged entities lack suitable transaction monitoring systems to detect linked transactions or if customers can repay loans through cash payments.

(b) Risk awareness:

See above on TF.

(c) legal framework and supervision/governance:

In addition to the other customer due diligence requirements of article 6 FM-GwG, AIs must in particular also have sufficient information regarding the origin of the customer's funds, for example in the case of loan repayments. They must also install appropriate transaction monitoring systems.

Conclusion: Based on the summarised scenarios of the SNRA, which suggest a medium vulnerability, the framework conditions presented mean that the vulnerability of consumer and small loans to being misused for the purposes of money laundering can be classified as low to medium.

Risk minimisation measures

The conclusion of credit agreements is reserved for credit institutions pursuant to article 1 para. 1 no. 3 BWG. As part of its supervisory activities, the FMA also focuses on the correct calibration of the transaction monitoring systems of obliged entities.

Total risk

In summary, the risk for TF is classified as medium to high and for ML as medium.

Recommendations

Further intensified cooperation between the authorities and stakeholders in order to highlight current patterns and trends and to take experience into account in the further development of the relevant legal bases.

Sector / Product / Service / Activity
Financial sector/ Mortgage loans
Mortgage loans are used to finance property by pledging the property to be purchased as collateral for the loan repayment. In the area of money laundering, the proceeds of criminal offences can be used for real estate investments, for example by using the proceeds for repayments or early redemption. In principle, it is also possible for terrorists or their supporters to use medium to long-term mortgage loans with large amounts to finance their activities.
Threat
Terrorism financing In the SNRA's summarised scenarios, the threat of mortgage loans being misused for terrorist activities was classified as a low risk. The use of mortgage loans for terrorist purposes is particularly difficult due to the link to a property, the associated entry in the land register and the long-term commitment and is hardly accessible to terrorists or their supporters.

Conclusion: To summarise, the threat can be classified as low.

Money laundering

In the SNRA's summarised scenarios, the threat was classified as high risk.

Mortgage loans can be used for money laundering in order to channel higher amounts of incriminated funds into the financial system through the purchase of (several) properties. Organised crime groups attempt to conceal the actual beneficial ownership and origin of the funds used to purchase properties, in particular through the use of forged documents and records. To minimise risk, it should be noted that AI must always be involved in the processing of mortgage loans. In addition, the involvement of notaries and lawyers is required for the contractual arrangements and entry in the land register.

Conclusion: In summary, the threat is classified as medium to high.

Vulnerability

Terrorism financing

The supervisory practice of the FMA and the available data and information do not indicate any particular vulnerability of the Austrian financial market.

Conclusion: Based on the summarised scenarios of the SNRA, which suggest a low vulnerability, the framework conditions presented mean that the vulnerability of mortgage loans to being misused for the purposes of terrorism financing can be classified as low.

Money laundering

In the summarised scenarios of the SNRA, the vulnerability of assets held with CIs/FIs with regard to misuse for money laundering purposes was classified as medium. The national vulnerability is to be derived below.

(a) Risk potential:

The number of new mortgage loans concluded has been declining since May 2022.

(b) Risk awareness:

Many smaller mortgage loans are taken out for the purchase of residential property for personal use. These are relatively small loan volumes. Large-volume - and in some cases purely speculative - property transactions in particular represent a higher risk.

(c) legal framework and supervision/governance:

In addition to the other customer due diligence requirements of article 6 FM-GwG, AIs must in particular also have sufficient information regarding the origin of the customer's funds, for example in the case of loan repayments. They must also install appropriate transaction monitoring systems.

Conclusion: Based on the summarised scenarios of the SNRA, which suggest a medium vulnerability, the framework conditions presented mean that the vulnerability of mortgage loans to being misused for money laundering purposes can be classified as medium.

Risk minimisation measures

The conclusion of credit agreements is reserved for credit institutions pursuant to article 1 para. 1 no. 3 BWG. As part of its supervisory activities, the FMA also reviews the transaction monitoring systems of obliged entities.

Total risk

In summary, the risk for TF is classified as low and for ML as medium.

Recommendations

Further intensified cooperation between the authorities and stakeholders in order to highlight current patterns and trends and to take experience into account in the further development of the relevant legal bases.

10 Sectoral risk assessment of the legal profession

General information
1.1. Number of professionals As at 31 December 2023, there were **7,073 lawyers** and **2,275 trainee lawyers** in Austria. **1.2. Areas of activity (business segment distribution ratio)** The lawyer is an advisor, counsellor or representative of his clients in all their public and private matters. According to the evaluation of a representative survey conducted among the members, in which, among other things, the proportion of the respective lawyer's activities was queried, **only 27% of the lawyer's business areas are** in the area of transactions subject to customer due diligence**; in contrast, 73% of the activities are not related per se** to financial and real estate transactions subject to due diligence. **1.3. Firm structure** The majority of lawyers work in **very small structures**. Half of all lawyers work as sole practitioners. A further quarter of lawyers work in small structures consisting of up to three lawyers. **1.4. Specifics of the legal profession** Lawyers have particularly strict training and authorisation requirements and are subject to a duty of confidentiality protected by fundamental rights. For more detailed information on the specifics, the general customer due diligence requirements under professional law and the duty of confidentiality, please refer to the explanations in the sectoral risk assessment.
Sector / Product / Service / Activity
The following implementation relates to the following products/services based on the catalogue of transactions subject to the customer due diligence requirements of article 8a RAO: • Purchase or sale of real estate (including escrow processing) • Purchase or sale of companies (including trustee handling) • Management of money, securities or other assets • Opening or managing bank, savings or securities accounts

- Establishment, operation, administration of trusts, companies, foundations or similar structures, including raising the funds required for the establishment, operation or administration of companies

A detailed analysis for the individual ML/TF-influenced products/services is carried out as part of the sectoral risk assessment.

General description

When **buying or selling real estate,** the activities of lawyers include legal advice, contract negotiations with the parties, drawing up the purchase contract, the fiduciary (step-by-step) handling of the exchange of the services to be provided by both parties, the self-calculation of taxes, obtaining any necessary permits (land transactions, forestry, property division, spatial planning, etc.) and the execution in the land register.

When **buying or selling companies,** the lawyers' activities include legal advice, contract negotiations with the parties, drafting the contracts, drafting the articles of association, if necessary the fiduciary (step-by-step) handling of the purchase price payment and the transfer of shares or assets, including further implementation measures, in particular obtaining any necessary approvals (land transactions; cartel court approval; approval under the Foreign Trade and Payments Act, etc.), self-calculation of taxes and implementation in the commercial register.

The **management of money, securities or other assets** regularly takes place in the capacity of (court-appointed) adult representative and insolvency administrator. Apart from this, the lawyer manages monetary assets almost exclusively in the context of liquidation trusts in connection with the purchase and sale of property or companies.

Bank, savings or securities accounts are generally opened or managed in connection with the execution of settlement trusts in connection with the sale of real estate and company shares, possibly in the context of board functions.

Lawyers are involved in the **establishment and operation of companies and private foundations** as part of their work. Furthermore, as members of the bodies of private foundations (executive board, advisory board), lawyers are involved in the management and administration of the foundation's assets, including the payment of benefits to beneficiaries; lawyers also fulfil supervisory board functions in companies and monitor the management by the executive board.

Threat

Terrorism financing:
The Supranational Risk Assessment (SRNA) categorised the threat of lawyers' services being misused for terrorist activities as a very high risk and stated that the TF threat assessment in relation to lawyers' legal services is considered in conjunction with ML. Threat scenarios include, for example, the provision of information through donations to non-profit organisations for which lawyers can act as advisors in the establishment of such

organisations. Possible, but not yet observed in practice, is the opening of accounts by lawyers, the use of lawyers as straw men in asset management or money transfers by lawyers via other accounts. Following this system, the Austria-specific threat situation for both points shows that it is not only the organisation of the legal profession in Austria and the applicable supervisory regime, but also a general increase in attention recently due to regular information about threat scenarios in the area of counter-terrorism, which means that the country-specific threat situation in Austria appears to be less severe than the classification made in the SRNA.

Conclusio:

The threat in the area of terrorism financing can be classified as low.

Money laundering:

In all transactions subject to customer due diligence, the threat of abuse for money laundering lies in the fact that the involvement of a lawyer or the processing of the transaction via a lawyer could create the appearance of harmlessness, legitimacy and respectability. Lawyers have a special position of trust in society and criminals can try to abuse lawyers by using them as a "seal of approval" for certain transactions.

Criminals may attempt to create complex and difficult to understand structures involving multiple jurisdictions, particularly offshore jurisdictions with disguised ownership. This often involves the owner of another company or legal structure being registered in a different jurisdiction. This combination of different legal services in different jurisdictions may be an attempt to deliberately add complexity to the transaction.

The acquisition of real estate or companies and company shares by persons domiciled or resident outside the EU/EEA poses an increased potential threat of money laundering. In such constellations, acquisition companies are often set up specifically for the purchase and are backed by numerous complex, nested legal entities. This can make it considerably more difficult to identify the beneficial owners and the origin of the funds in Austria. Similar risks also exist when setting up (acquisition) companies for the purpose of managing assets (such as shareholdings).

In contrast, the threat scenario in connection with the opening and management of bank, savings and securities accounts or trusts, foundations and similar structures by lawyers is considered to be lower. Lawyers working in Austria are particularly sensitive to the issues of money laundering, terrorism financing and proliferation.

Conclusio:

The professional and general framework conditions mean that the threat can be categorised as medium to high.

Proliferation financing

Threats exist due to Austria's historically close business contacts with Iran. In the past, arms deliveries were also made to Iran, which led to the tightening of the relevant control

regulations and can no longer be carried out today. Austria also has a strong financial system with international connections that could be vulnerable to proliferation financing. Structures involving third countries that serve to circumvent sanctions are conceivable.

With regard to North Korea, the main theoretical risks are the circumvention of sanctions by third parties and trade in illegal goods to finance proliferation. There are also reports of sports clubs that have contacts with the North Korean regime.

However, there are no known specific threat scenarios for the legal profession. As a rule, lawyers are not involved in the above-mentioned structures, especially as these are not part of their usual fields of activity.

Conclusio:
To summarise, the threat in connection with proliferation financing can be classified as low.

Vulnerability

Terrorism financing:
The assessment of vulnerability to terrorism financing in connection with legal services provided by lawyers is generally considered in conjunction with money laundering schemes designed to conceal the illegal origin of the funds.

It should be noted that there is a probability that the purchase or sale of real estate will be misused for terrorism financing. However, additional elements, such as the transfer of the sales proceeds to dubious organisations, corresponding states or corresponding persons, would have to be added. As a rule, however, the lawyer is not involved in this.

The involvement of a lawyer in the purchase and sale of companies for terrorism financing purposes is also rather atypical, as terrorism financing usually requires liquid funds quickly and sustainable investments in companies are therefore not suitable for terrorism financing purposes. In the case of corporate transactions, further circumstances would therefore have to be added, in particular with regard to the forwarding of sales proceeds to the corresponding recipients, in which lawyers are not involved or which are no longer part of the (typical) corporate transaction.

Conclusio:
Based on the SRNA, which suggests a high vulnerability, the framework conditions described lead to the vulnerability of lawyers to being misused for the purposes of terrorism financing being classified as medium.

Money laundering:
In the summarised scenarios of the SRNA, the vulnerability of lawyers with regard to abuse for the purposes of money laundering was classified as high. The national vulnerability is to be derived below:

(a) Risk potential:
As lawyers are often organised and operate in small structural units, perpetrators may see an opportunity for a lack of sensitivity and vigilance in ML risks. It is also possible that lawyers are involved in the management of complex legal situations and that the behaviour of clients triggers "red flags" that are still rather unknown.

(b) Risk awareness:
There is a high level of risk awareness in the legal profession (lawyers, trainee lawyers, employees and bar associations). The bar associations are obliged to check their members' compliance with the provisions of article 8a ff RAO and take a variety of steps to monitor their members' ML/TF obligations. On the one hand, the bar associations check off-site by means of a questionnaire and, on the other hand, during on-site inspections whether lawyers, trainee lawyers and law firm staff comply with the legal provisions regarding the prevention of ML/TF. In addition, compliance with the legal provisions (e.g. with regard to beneficial ownership) is also checked as part of the client money and fiduciary audit. Among other things, it is checked whether a written law firm risk assessment is available and which strategies are derived to prevent ML/TF (e.g. law firm guidelines, employee training, appointment of a money laundering officer, etc.). In the last four years (2020 - 2023), an average of 30.55% of all lawyers throughout Austria were audited annually.

In the course of the on-site audits, checks are carried out to determine whether the identity of the parties and beneficial owners of money laundering-related transactions have been established and documented, whether suspicious activity reports have been submitted and whether the corresponding documentation is available. These checks are carried out both on a random basis and with regard to the specific risk profile of a law firm; in addition, of course, they are also carried out on an ad hoc basis if there are grounds for suspicion. The audit results show that the legal requirements are complied with as far as possible and, in particular, that the identification of beneficial ownership is practically seamless.

(c) legal framework and supervision/governance:
It should also be noted that, in addition to the lawyer, other obliged entities and authorities are regularly involved in the conclusion and settlement of a transaction. As a rule, this does not lead to any neglect of the obligations incumbent on lawyers to prevent money laundering and terrorism financing, but rather means that special attention is paid to these obligations; This is because negligence in the fulfilment of one's own obligations harbours the considerable risk that this will come to light when another person/institution involved in the system for combating money laundering and terrorism financing (such as a credit institution) independently fulfils its obligations and that this could result in considerable disadvantages for the lawyer who neglects his obligations. The same applies to the supervision exercised by the Bar Association, in view of which every lawyer is aware that money laundering checks are to be expected in any case. This also significantly increases sensitivity in this area.

For example, property transactions require an entry in the land register kept by the court. In addition, the calculation and payment of property income tax, real estate transfer tax and registration fees must be carried out, including the corresponding reports to the tax authorities.
This self-calculation by the representatives of the parties is also in the interests of the tax authorities in particular, as it significantly reduces their workload. The tax authorities then check whether the self-calculation has been carried out correctly by means of special tax audits (external audits).

In the case of property transactions with buyers from third countries (foreign property acquisitions), the authorities also check the beneficial ownership. It is particularly important that the payment flow, insofar as it is made via bank accounts - as is usually the case - is also and especially checked at bank level; in addition, the processing of monetary transactions is carried out via the trustee organisations of the bar associations, which are authorised to inspect them as part of their supervision.

Finally, a property transaction requires notarisation, which involves an additional identity check of the persons involved by the notary.

The legal framework corresponds to the current status of the EU Money Laundering Directives. Compliance with organisational measures (in particular risk assessments, training and structured processes) in the law firm ensures that ML/TF risks are adequately taken into account when accepting new clients, accepting mandates and managing ongoing business relationships.

Supervision of the legal profession in the ML/TF area is carried out by the nine bar associations, which carry out regular, risk-based and ad hoc inspections. Supervision includes not only the review of individual mandates, but also compliance with organisational measures in the law firm. Violations can result in far-reaching disciplinary sanctions.

Human and financial resources:
In 2023, a total of 145 people in the nine bar associations were involved in supervision in connection with the prevention of ML/TF.

Conclusio:
Based on the summarised scenarios of the SRNA, which in themselves suggest a high vulnerability, the framework conditions presented mean that the vulnerability of lawyers to being misused for the purposes of money laundering in Austria can be classified as medium.

Proliferation financing

(a) Risk potential:

Similar to vulnerability in the context of money laundering, it can be stated that offenders are often organised and operate in small structural units, so that they see an opportunity in a lack of sensitivity and vigilance.

(b) Risk awareness:
Nevertheless, there is a high level of risk awareness in relation to the countries typically affected, Iran and North Korea, as well as in relation to dual-use goods. Lawyers deal with the risks that affect them and must also take these into account in their risk assessments. For some time now, the ÖRAK has maintained its own website on sanctions[11] and regularly provides information on the relevant legal acts.

(c) legal framework and supervision/governance:
The Lawyers' Act contains provisions (in particular article 8a (9) and (10) RAO) for the implementation of Recommendation 1 of the "FATF Recommendations" on the implementation of strategies, procedures and controls for the identification, assessment, monitoring, management and mitigation of proliferation financing risks. Explanations within the framework of the guidelines are already in preparation. Compliance with these regulations is checked as part of the money laundering controls.

Human and financial resources:
In 2023, a total of 145 people in the nine bar associations were involved in supervision in connection with prevention.

Conclusion: In summary, the vulnerability can be classified as medium.

Risk minimisation measures

In addition to the risk-mitigating measures already mentioned above, the following measures should also be mentioned, which further minimise the risk pro futuro:

- The risk-based approach to the supervisory measures of the bar associations will be further strengthened and automated.
- Increased individual case analyses by the chambers: It should be taken into account that the evaluations and assessments of the risk assessments of the individual professionals are increasingly being incorporated into supervision in terms of both content and organisation
- the findings from supervisory activities are also specifically taken into account in the area of further training;
- Violations of professional regulations may result in severe disciplinary consequences;
- Law firm-specific risk assessment and mandate-specific review.

[11] Available in the internal area at https://www.oerak.at/mitglieder/informationen/sanktionen/.

- Increased networking and cooperation with other bodies and obliged entities: First and foremost, the FIU (Money Laundering Reporting Centre) and the already established register of beneficial ownership. Lawyers are authorised to inspect the register in accordance with article 9 WiEReG. In particular, the findings from networking with the FIU flow directly into the information provided to lawyers and training courses;
- Reference should also be made to the security instruments associated with the settlement trusteeship (trust register, settlement via recognised credit institution).

Total risk

The overall risk is categorised as low to medium.

Recommendations

- Continuation of training and further education measures as well as sensitisation in the profession.
- Continuation of the intensified cooperation between the legal profession and other authorities involved, in particular the BMJ, BMF and BMI/ Money Laundering Reporting Centre as well as the ÖNK.
- Expansion of automation for increased off-site inspections by the bar associations.

11 Sectoral risk assessment notaries

General information
1.1. General information There are 536 notary offices in Austria (as of 10 March 2025), with 529 notaries and 669 notary candidates. Around 81% of the offices are run as individual notary's offices, around 19% as partnerships. Austrian notaries are, in principle, generalists. This means, on the one hand, that every notary can provide the same legal services and therefore covers all of the fields of activity described below and, on the other hand, that notaries are authorised to exercise their powers throughout Austria. The legally defined scope of the profession includes the following activities: **Preparation of public deeds; drafting of private deeds/party representation; fiduciary services; mediation; court commissioner's office.** **1.2. Specifics of the occupational group** Austrian notaries are freelance lawyers who advise their clients and draw up contracts and public deeds. They are mainly active in the non-contentious and preventive legal field and hold the official title of public notary. Their activities are primarily characterised by their independence and partly sovereign functions (e.g. in the course of the court commission in the fulfilment of judicial tasks and in the preparation of public deeds). In contrast to lawyers, notaries, as holders of a public office, have a duty to instruct all parties and must protect the interests of all parties equally. They may not participate in prohibited, suspicious or fictitious transactions (§§ 5 para. 3, 34 NO). In their work, notaries are subject to strict professional and disciplinary regulations of the Notarial Code and the Directives of the Austrian Chamber of Notaries (ÖNK) and must exercise a high degree of care. The highest level of supervision is exercised by the Federal Minister for Justice, while the presidents of the courts of first and second instance supervise the conduct of the office. The Chamber of Notaries (NK, § 153 NO) is responsible for direct professional supervision. New notary positions can only be created or relocated by Regulation of the Federal Minister of Justice. **1.3. Analysis of the domiciles of the parties (settling parties)** An analysis of the residences of the parties (fiduciaries) of the notaries for 2023 shows that the parties are predominantly from Austria (95.40%). The distribution also revealed the following: EU/EEA area (99.24%) and non-EU/EEA area; of which 0.43% are already derived from Switzerland. The remaining non-EU/EEA countries are: United States of America, United Kingdom, Canada, United Arab Emirates and Australia. With regard to the high-risk third countries covered by the European Commission's Delegated Regulation (EU) 2016/1675, no participations in notarial business activities were identified for 2023.
Methodology
2.1 Products - AML/CFT/PF relevant services In their function as generalists, notaries practise in various business areas.

According to § 36a NO, the notary "is *obliged, in view of the particularly high risk of money laundering (§165 StGB) or terrorism financing (278d StGB), to examine with particular care all transactions in which he carries out financial or real estate transactions in the name and for the account of his party or participates in their planning or execution for his party and which relate to the following:*

1. *the purchase or sale of property or companies,*
2. *the management of money, securities or other assets, the opening or management of bank, savings or securities accounts, or*
3. *the establishment, operation or management of trusts, companies, foundations or similar structures, including the procurement of the funds required for the establishment, operation or management of companies."*

According to a survey in 2021, 46% of notarial business activities qualify as "money laundering-related transactions" within the meaning of article 36a NO, while 54% of notarial business areas had no connection to "money laundering-related transactions".
For this reason, the Professional Law Amendment Act 2024 (BRÄG 2024) aimed to expand and sharpen the profile of notaries as generalists accordingly. article 36a para. 5 NO now also includes the area of proliferation financing and sanctions regimes. Corresponding attention is now required in the risk assessment of the notary's offices: *"(...) To this end, a risk assessment shall be prepared and strategies, controls and procedures shall be put in place to mitigate and manage the risk of non-implementation and circumvention of targeted financial sanctions related to proliferation financing. (...)*"

2.2.1 The "settlement trust"

The majority of money laundering-related transactions in which notaries are involved in a payment transaction are processed by means of notarial trusteeship (in order to ensure step-by-step processing by the notary to protect the interests of the buyer and seller), which must be entered in the Trustee Register (THR) of the ÖNK from a trust amount of € 10,000. In practice, the trusteeship product is almost always associated with money laundering-orientated real estate and company law transactions.
Number of registrations in the THR: 51,502 (2021), 43,582 (2022), 34,157 (2023) and 37,439 (2024).
The average amount (total framework) of a trust was € 337,601.00 (2021), € 352,877.00 (2022), € 325,663.00 (2023) and € 320,972.00 (2024). The average number of settlors involved in a trust was as follows: 2.94 (2021), 2.95 (2022), 2.88 (2023) and 2.90 (2024).

The following trust accounts were opened by notaries at **Notartreuhandbank AG** (NTB), currently the only credit institution authorised and recognised to process notarial trusteeships: 57,074 (2021), 47,205 (2022), 40,492 (2023) and 43,393 (2024). In 2023 and 2024, these were opened for an average period of around three months.

2.2.2 Audits, training and information measures

The NCPs are obliged to regularly audit the files, business registers, books, directories, collections and the business operations of notaries as a whole (§ 154 para. 1 NO, "Audit"). In particular, it must be monitored whether the notaries comply with the provisions that serve to prevent or combat money laundering (ML), terrorism financing (TF) or proliferation financing (PF). In cases

of suspicion, unannounced interim or special audits are also carried out by the NK (extraordinary audit). If the notarial chamber conducting the audit discovers a deficiency or violation in the course of its audit or on another occasion, it must issue an appropriate reminder, depending on the severity of the offence, conduct disciplinary proceedings or initiate disciplinary proceedings through the Higher Regional Court as the designated disciplinary court. If the NK comes across facts relating to AML/CFT/PF, it must also submit a suspicious activity report to the Money Laundering Reporting Centre (article 36c (1) NO). On average, each notary's office is audited at least once every three to five years (85 (2021), 173 (2022), 86 (2023) and 78 (2024) office audits, Austria-wide).
The ÖNK offers numerous seminars on the topic of preventing and combating AML/CFT/PF that are in high demand: ten seminars were held in 2021, nine seminars each in 2022 and 2023 and 22 seminars in 2024.
Since 2008, the Austrian Chamber of Notaries has provided its members with regularly updated guidelines on the prevention of money laundering and terrorism financing (ML/TF) in electronic form and informs them of important innovations by means of circulars/circulars.

Product-specific risk assessment

Non-financial sector, point 10 "Legal services from notaries and other independent legal professions" of the SNRA SWD (2022) 344 (page 194 et seq., hereinafter summarised under the term *legal services*).

General description

In accordance with Art. 2 para. 1 no. 3 lit. b of Directive (EU) 2018/843, the SNRA (page 198) and, in future, Art. 3 para. 3 lit. b of Regulation (EU) 2024/1624, notarial services in Austria include the following areas (money laundering-related transactions pursuant to article 36a NO, see also point 2.1):
Purchase/sale of real estate: As part of their activities under both § 1 NO and § 5 NO, notaries are involved in the purchase of real estate for their clients (legal advice, drafting of contracts, notarisation of signatures, execution in the land register, assessment and collection of fees under tax law).
Purchase/sale of companies: As part of their activities under both § 1 NO and § 5 NO, notaries are involved in the acquisition of companies for their clients (legal advice, drafting of contracts, notarisation of signatures, assessment and collection of fees under tax law).
Management of money, securities or other assets: The management of money, securities and other assets by notaries is generally possible within the framework of § 5 NO. In practice, the administration of money, securities and other assets by notaries is predominantly carried out as a court-appointed curator or as part of the activity as a (court-appointed) adult representative or authorised representative for persons who are not capable of making decisions.
Opening or managing bank, savings or securities accounts: The opening of bank accounts is possible in particular in connection with the purchase/sale of real estate and the purchase/sale of companies, whereby the accounts in these cases are always trust accounts (escrow accounts) for the settlement of the respective transaction. For these accounts, which may only be held at a specially recognised credit institution (see point 2.2.1. above), there is a close-knit professional and supervisory network. In addition, it is possible to open or manage bank, savings or securities accounts as part of the management of money, securities or other assets. In this case, these are

usually accounts that are managed as a curator or judicial adult representative and are therefore subject to judicial control. Finally, it is possible to open a bank account for the safekeeping of money (§ 5 and § 104ff NO). Accounts pursuant to article 104 NO (these can only be opened on the occasion of the recording of a notarial deed for the safekeeping of money and subsequent delivery to a specific recipient on behalf of the party or for deposit with the authorities or the court) are generally opened for deposit with the court and are therefore of no interest to offenders. They hardly play a role in practice. Apart from the points mentioned above, notaries are generally not involved in the opening or management of bank, savings or securities accounts.
Establishment, operation, administration of trusts, companies, foundations or similar structures, including raising the funds required for the establishment, operation or administration of companies: In particular, the opening and administration of trusts is not relevant, as Austria has not ratified the Hague Trust Convention and trusts have no practical relevance. In Austria, there are foundations under the Private Foundations Act (PSG). According to article 1 (1) PSG, private foundations are legal entities to which assets are dedicated by the founder in order to serve the fulfilment of a permitted purpose determined by the founder through their use, administration and realisation; they enjoy legal personality and must have their registered office in Austria. Private foundations must also be entered in the commercial register and in the register of beneficial ownership. As part of their activities under both § 1 NO and § 5 NO, notaries are involved in the formation of companies and foundations for their clients (also on the basis of statutory formal requirements) (legal advice, drawing up and, if necessary, amending association's statutes, filing applications with the commercial register, participation in any reorganisations). Usually, the notary is also involved in the planning and/or implementation of a company in the function of representing the parties to a company or when notarising signatures, for example when appointing the management. Due to professional law, notaries are subject to strict regulations regarding the exercise of their profession and any secondary activities. According to Art. I Z 7 of the STR 2000, the notary must notify the competent chamber of notaries of any paid secondary activities. In addition, § 7 para. 2 NO stipulates that the notary is prohibited from any activity that is incompatible with the honour and dignity of the profession.

Threat

Terrorism financing

In the summarised scenarios of the SNRA, the threat of misuse of legal services is generally classified as very significant for both terrorism financing and money laundering due to the methods identified for concealing the illegal origin of financial resources (see SNRA SWD (2022) 344, page 195f). This assessment is not valid, as the assets used in money laundering always originate from criminal offences, whereas in terrorism financing, legal funds can also be used, with the focus being on the use of funds. It therefore makes sense to consider terrorism financing, money laundering and money laundering-related transactions separately in accordance with Art. 2 para. 1 no. 3 lit. b of Directive (EU) 2018/843, the Notarial Code and, in future, Art. 3 para. 3 lit. b of Regulation (EU) 2024/1624.

In all money laundering-related business areas, the **threat of abuse for terrorism financing** lies in the fact that the involvement or processing of the transaction via notaries could suggest harmlessness, respectability and creditworthiness. If bank accounts are involved, there could also be a risk that banks will scrutinise notaries less strictly as account holders. When buying/selling

property or companies, a classic threat scenario could be an attempt by perpetrators to obtain assets for terrorism financing purposes by investing in the property sector (e.g. through profitable investments). However, classic threat scenarios in the area of terrorism financing could also include attempts to use notaries as "front men" for asset management, the opening of donation accounts as a cover for collecting money and the establishment and management of companies in order to generate funds for terrorism financing.

Conclusio:
To summarise, the threat in the area of terrorism financing can be classified as low (lowly significant).

Money laundering:
In all business areas susceptible to money laundering**, the threat of abuse for money laundering** lies in the fact that the involvement or processing of the transaction via notaries could suggest harmlessness and respectability. If bank accounts are involved, there could also be a risk that banks will scrutinise notaries less strictly as account holders. When buying/selling property or companies in the money laundering sector, a classic threat scenario could be an attempt by perpetrators to conceal the origin of illegally obtained assets by investing in the property sector or to make large-scale company acquisitions. The illegal origin of high proceeds from criminal activities could be concealed "in one fell swoop" and thus "laundered clean". Through such investments, the creditworthiness of acquired companies could also be utilised for further criminal activities (e.g. through borrowing). In the area of money laundering, classic threat scenarios could consist of perpetrators attempting to set up companies with the help of notaries in which "straw men" are used as shareholders and/or managing directors to conceal the origin of assets or beneficial ownership, or in the transfer of shell companies for the same purpose. In addition, the purpose of managing money, securities or assets, opening or managing bank, savings or securities accounts and setting up companies or foundations may be to conceal illicit funds through financial transactions or the establishment of entities, or to conceal beneficial ownership through complex constructions. Another threat scenario could also be posed by bogus companies that seek to conceal the illegitimate origin of assets through strategic property investments or large-scale company acquisitions, or that are set up for the purposes of social and tax fraud. In this case, there could be a risk of attempts to use notaries to set up companies or transfer shares.

Conclusio:
To summarise, the threat in the area of money laundering can be classified as medium to high (moderately significant to significant).

Proliferation financing
In all business areas at risk of proliferation financing, the **threat of abuse is** that the involvement or processing of the transaction via notaries could give the impression of harmlessness and respectability. If bank accounts are involved, there is also a risk that banks will not scrutinise notaries as account holders as strictly, which could facilitate misuse to finance the proliferation of weapons of mass destruction. Classic threat scenarios for notaries in the context of proliferation financing include attempts to use them to process transactions that serve to finance the proliferation of weapons of mass destruction. In this case, there could be a risk of attempts

to use notaries to set up companies or foundations that are used as a cover for the transfer of funds - especially with regard to high-risk countries such as the Islamic Republic of Iran or the Democratic People's Republic of Korea (DPRK). The opening and management of bank accounts via notaries can also be misused to disguise the origin and intended use of the funds, thereby concealing the actual intention.

Conclusio:
To summarise, the threat in the area of proliferation financing can be classified as low (lowly significant).

Vulnerability

In the summarised scenarios of the SNRA, the vulnerability of legal services in the areas of terrorism financing and money laundering is uniformly classified as high (significant). As there are no substantive differences in the notarial sector in terms of risk potential, risk awareness and legal framework/supervision/governance, a uniform assessment of vulnerability is made - as in the SNRA. The area of proliferation financing is also included in the assessment.

(a) Risk potential: In the areas of buying/selling property and buying/selling companies, a large number of transactions, some with high volumes, are carried out by notaries every year (see point 2.1. above). In addition, property prices have risen sharply in some cases due to the COVID-19 pandemic. Overall, Austria is also "popular" with criminals due to its humane prison conditions, which could increase the risk of criminal activity.

(b) Risk awareness: There is a high level of risk awareness throughout the profession (notaries, notary candidates, employees and chambers), which is due in particular to the large number of risk minimisation measures: Notaries are obliged to prepare and continuously update a personal risk assessment. With the inclusion in the BRÄG 2024, the area of proliferation financing is now also comprehensively taken into account. The ÖNK also regularly prepares a sectoral risk analysis for the notarial profession, which, like the National Risk Assessment and SNRA, is included in the personal assessment of notaries. The ÖNK and the chambers of notaries as supervisory authorities implement comprehensive measures in the area of training and sensitisation. Regular and effective supervisory measures are carried out by the chambers of notaries (office audits pursuant to article 154 NO), in which compliance with money laundering / terrorism financing / proliferation financing obligations is checked in particular. If violations of professional regulations are found, there are strict disciplinary consequences (see article 158 NO). In addition, the BRÄG 2024 introduces risk-based supervision, which aims to deploy the resources and measures of the supervisory authorities in a more efficient and targeted manner. This approach focuses on the identification and assessment of risks associated with money laundering, terrorism financing and proliferation financing.

(c) Legal framework and supervision/governance: It should also be noted that in Austria, in addition to notaries, other professional groups, authorities and courts obliged to prevent money laundering, terrorism financing and proliferation financing are involved in notarial services. For example, in the case of property transactions, the underlying titles (deeds) are checked by the land registry courts before entry in the court-registered land register (§ 26 GBG). The tax

authorities are involved with their inspection mechanisms, in particular as the register authority of the register of beneficial owners and through the calculation and payment of taxes and fees (ImmoESt, GrESt, registration fee). Insofar as notaries carry out self-calculation, this is done in the interests of the tax authorities and is also verified by them by means of special tax audits; the notaries take on a quasi collection function for the Republic of Austria. In the case of property transactions with buyers from third countries (foreign property acquisition), the acquiring third-country company or the domestic acquisition company established for this purpose must report its beneficial owners to the register of beneficial owners. The transaction is also scrutinised by the land transfer authorities. Pursuant to article 11 para. 1 WiEReG, notaries must also ensure that the acquiring third-country company has reported its beneficial owners in accordance with article 5 WiEReG before notarising or recording a notarial deed for the purpose of acquiring a property located in Austria, which ensures that the beneficial owners are recorded in any case. Every payment via accounts involves a bank, which in turn is subject to the strict provisions of the FM-GwG. In the case of notarised transactions, there is also a strict recognition procedure for which banks notaries are allowed to hold accounts and deposit client funds. Currently, only the Notary Trust Bank (NTB) exists, which, in addition to other security measures, must comply with a same-day notification system for all parties involved in a transaction.

Human and financial resources:
In 2024, a total of 166 people at the Austrian Chamber of Notaries and the six chambers of notaries were involved in the topic and supervision in connection with the prevention of AML/CFT/PF.

Conclusio:
Based on the summarised scenarios of the SNRA, which suggest a high level of vulnerability (significant), the national and (for the areas of terrorism financing, money laundering and proliferation financing identical) internal professional framework conditions described above mean that the vulnerability of notaries to being misused for the purposes of terrorism financing, money laundering or proliferation financing can be classified as medium to high in the area of money laundering and as medium in the area of terrorism financing and proliferation financing.

Risk minimisation measures

In addition to the risk-mitigating measures already mentioned above under risk awareness, the following future measures should be mentioned, which will also further minimise the risk pro futuro:

- The risk-based approach to the supervisory measures of the chambers of notaries is constantly being strengthened. Among other things, a significant step towards the further development and organisation of risk-based supervision was taken as part of the BRÄG 2024 through amendments to articles 82, 109a, 112, 113 and 140d NO. The Directive of the Austrian Chamber of Notaries on Risk Factors for the Prevention of Money Laundering, Terrorism Financing and Proliferation Financing (Rf-RL) is of central importance here. These Directives supplement risk-based supervision by defining specific criteria and indicators that support notaries in identifying and assessing risks. The personal risk assessments are reviewed regularly.

- The knowledge gained from risk-based supervision is increasingly being incorporated into basic and advanced training; special auditor training courses are to become standard.
- The Federal Ministry of Finance has included foreign legal entities (companies, foundations and comparable legal entities whose registered office is not in Austria or another Member State) in the scope of application of the WiEReG. If these foreign legal entities wish to acquire ownership of a property located in Austria, they are deemed to be foreign legal entities subject to reporting requirements, which must register in the supplementary register for other legal entities before notarising or recording a notarial deed for the purpose of acquiring a property located in Austria and then report their beneficial owners. Before notarising or recording a notarial deed for the purpose of acquiring a property located in Austria, notaries must ensure that foreign legal entities, trusts and trust-like arrangements whose administration is not located in Austria or in another Member State have reported their beneficial owners. The obligations of the legal entities concerned are subject to severe penalties (financial offences of up to EUR 200,000).
- The increased cooperation (administrative assistance) between the Austrian Chamber of Notaries and other stakeholders in the area of preventing money laundering, terrorism financing or proliferation financing will further reduce the risk. In particular, there is a regular exchange within the framework of a separate public-private partnership ("PPP") between the BMI, the Money Laundering Reporting Unit (A-FIU) and the BMJ, whereby the A-FIU must provide notaries with access to current information on methods of money laundering and terrorism financing as well as on indications by which suspicious transactions can be recognised; the A-FIU must also provide notaries with timely feedback on the effectiveness of suspicious activity reports and the measures taken as a result (article 37 (9) NO).

Total risk

Taking into account the existing (see Risk awareness) and future risk mitigation measures, the overall risk for terrorism financing and proliferation financing is classified as low to **medium** (lowly significant to moderately significant) and for money laundering as **medium** (moderately significant).

Recommendations

- Continuation of the intensified cooperation between the notary's office and other authorities involved, in particular the BMJ, BMF and BMI/ Money Laundering Reporting Centre.
- Continuation of training and sensitisation of the profession.
- Expansion of risk-based supervision, establishment of a central staff unit at the Austrian National Audit Office for the coordination of supervisory measures and training of auditors in order to round off the necessary internal professional know-how with specialist know-how on the prevention and detection of money laundering, terrorism financing or proliferation financing.

12 Sectoral risk assessment of tax consultants and auditors

General description
General information on the sectors: **General information on the activity** The professional groups of tax consultants and auditors fall into the category of the non-financial sector as liberal professions in the field of economic and legal advice and representation. Tax consultants provide services for companies, in particular for the legal recording of company figures in accounting and represent their clients in dealings with tax authorities, social security institutions and other authorities. Auditors primarily provide auditing services to check the accuracy and legality of financial and non-financial company information. Tax advisors and auditors are only directly involved in financial transactions in exceptional cases; at most, they only play a direct role in financial transactions when acting as trustees, which is not part of the core activity of these professions. On the one hand, their activities and services are likely to be misused for the purposes of money laundering and terrorism financing; on the other hand, they can gain detailed insights into the structures and finances of their clients, especially with regard to companies. This enables tax advisors and auditors to obtain a picture of the origin of income and the beneficial owners and possibly recognise any anomalies. With regard to the prevention of money laundering and terrorism financing, they primarily have an indirect and retrospective "observer role", as the activities primarily relate to the processing of transactions that have already been carried out. Pursuant to article 77 (6) WTBG 2017, tax advisors and auditors are authorised to consider the information and documents provided to them by the client, in particular figures, to be correct and complete. Audit engagements and other engagements that require impartiality and independence may only be carried out after conscientiously ascertaining the accuracy of the facts and circumstances to be confirmed. This means that, as with other consultancy professions, they can only play a role in the prevention of money laundering and terrorism financing where their services are involved in the preparation of business cases or transactions and therefore provide "money laundering-related" services. **Number of professionals and total turnover** As of December 2024, there are a total of 12,125 holders of professional licences in the areas of tax consulting and auditing in Austria. This can be further broken down into 8,525 natural persons and 3,600 companies (corporations and partnerships). As of December 2024, there are a total of 9,061 authorised tax advisors in Austria. Of these, 6,464 are natural persons and 2,597 are companies. As of December 2024, there are a total of 3,064 authorised auditors in Austria. Of these, 2061 are natural persons and 1003 are companies.

The calculated total turnover of all tax consultants and auditors in Austria was around 3.6 billion euros as of 2023.

Firm structure

Tax consultants and auditors utilise a wide variety of law firm structures in the performance of their work. These range from small one-person law firms to large law firm networks with up to over 1000 employees. Employees are not only professionals and trainees, but also people who take on front and back office activities or act in an organisational and system-maintaining capacity in the law firms.

The size of law firms in Austria is broken down by the number of employees as of 2022 as follows

- around 85% - law firms with fewer than ten employees
- around 14% - law firms with 10 - 50 employees
- around 1% - law firms with over 50 employees.

Number of clients

Tax consultants and auditors work for a large number of clients. Clients are primarily companies from a wide range of business sectors, but also private individuals from all professional fields.

As of 2019, the number of clients per law firm in Austria is statistically distributed as follows

- Around 41% of law firms look after up to 100 clients,
- around 42% look after up to 500 clients,
- around 11% look after up to 1000 clients,
- and around 6% of law firms have more than 1,000 clients.

Duty of confidentiality (legal privilege)

Tax advisors and auditors are subject to a statutory duty of confidentiality (article 80 WTBG 2017) due to the strictly confidential relationship with their clients within the scope of their professional activities. Due to this statutory duty of confidentiality, they are entitled to refuse to testify as a witness in legal proceedings. However, this duty of confidentiality does not apply pursuant to article 80 para. 4 WTBG 2017 if and to the extent that reporting and information obligations exist under the provisions of EU Directive (EU) 2018/843 and the associated implementing measures.

Threat

Money laundering and terrorism financing

As in the Supranational Risk Assessment, we would like to point out that the assessment of the terrorist threat in connection with the services of auditors and tax advisors was examined together with money laundering. The threat of terrorism financing therefore does not require a separate assessment.

In the summarised scenarios of the Supranational Risk Assessment, the threat of tax advisors and auditors being misused for money laundering and terrorist activities was classified as a significant risk. The national threat will be derived below.

As stated in the Supranational Risk Assessment, service providers (which the Supranational Risk Assessment includes the services of accountants, auditors, consultants and tax advisors) remain at risk of being infiltrated or owned by organised crime groups and used by them to launder illicitly generated proceeds. Criminals can take advantage of their advisory services and expertise

in the creation and management of structures, as well as the ability to provide documentation and assurances in relation to business activities. The reputation associated with certain professions makes them attractive targets for money launderers, as does the use of client accounts. The Supranational Risk Assessment assumes that professionals may be unwittingly involved but could also be collaborating with criminals or wilfully neglecting their duties to combat money laundering and terrorism financing.

The services provided by tax advisors and auditors primarily serve to ensure compliance with statutory regulations. The lawful execution of assignments is a statutory professional duty of the profession. Nevertheless, the services can also be used or misused to support a variety of money laundering schemes. Possible threat scenarios must be considered in terms of the objective and timing of the predominant fiduciary services on the one hand, and whether a scenario is likely to lead to abuse for ML/TF purposes on the other. In Austria, tax advisors in particular are authorised to carry out a large number of activities that are also open to other legal advisory professions, but for which - due to a lack of risk propensity - there are no prevention obligations. Therefore, significant threat scenarios of this kind are generally unlikely to arise when carrying out such activities. In addition to material assistance, support and advice in tax matters, threats may therefore generally relate to scenarios in connection with the execution of financial or real estate transactions in the name and for the account of their clients or the involvement in the planning and execution of transactions concerning the purchase and sale of real estate or commercial enterprises, the management of their clients' assets, the opening of accounts or the procurement of funds required for the establishment, operation or management of companies. Insofar as tax advisors and auditors are authorised to provide such services at all, these services are not part of the core activities of the professionals, meaning that threat scenarios relating to them are of secondary importance. In the case of essential core activities of the professions - legally compliant preparation of accounts and their auditing - threat scenarios for the purposes of ML/TF or their prevention must be considered from the point of view that these activities are downstream of both the realisation of predicate offences and the concealment of assets obtained from them. It is therefore not only difficult to take preventive action, but at least insofar as the circumstances are closed in time and no permanent criminal activity is involved, the obligations within the scope of customary professional activities in specific threat scenarios may possibly lead to subsequent detection, which, however, is not the subject of the obligations to prevent abuse.

Based on an analysis of data from the crime statistics of the general criminal investigation department from 2020 to 2023, the offences that were most frequently investigated (not convicted!) in connection with the basic offence of money laundering can be determined. Accordingly, the predicate offence is very often linked to fraud, often in connection with document offences. Fraud now mainly takes place on the internet, with forged documents occurring particularly frequently in connection with the online opening of bank accounts using the video identification procedure. In the tax consultancy and auditing services sector, it has not yet been possible to observe that these two main risk groups of fraud and document offences in the form described are highly relevant to the work of a tax consultant or auditor, so no significant threat can be assumed in this respect.

The analysis of the crime statistics and the SARs submitted to the A-FIU also shows that financial offences can regularly constitute predicate offences to money laundering. In 2023, 15% of the suspicious activity reports received by the A-FIU were classified as tax evasion offences (mainly bogus companies). The conviction figures also show that predicate offences under financial criminal law can pose a constant threat. According to previous experience, tax evasion as a money laundering offence occurs primarily in connection with bogus companies and constructs in the construction and service industries. The bogus companies are used to withhold social security contributions on a large scale and to evade taxes.

Example: Cleaning company

Cleaning companies that do not comply with the law can be recognised, for example, by the lack of a business registration, incomplete or incorrect certifications such as ISO 9001 or the absence of public liability insurance. Other indicators can be the non-payment of social security contributions, working without bank processing, bogus self-employment or employing unregistered or only marginally registered workers. Indications may also include unusually low prices, non-transparent invoices (e.g. no detailed description of the services or the absence of a VAT number) and the lack of safety clothing or tested chemicals. High labour turnover, incomplete information on the homepage or the lack of an imprint also indicate irregularities. In addition, invoices are often paid in cash.

As such sham companies are usually characterised in particular by the non-fulfilment of tax obligations, the tax advisory and auditing services sector rarely comes into direct contact with sham companies. Fictitious companies do not regularly use the services of tax advisors and auditors, meaning that the proactive involvement of persons entitled to exercise the profession in fictitious company constructs has not been observed to date. Nevertheless, this threat scenario must be included in the measures to combat money laundering, terrorism and proliferation financing, because clients of persons authorised to exercise the profession may have business relationships with bogus companies and, in this context, a contribution can be made to the detection of bogus companies if there are corresponding suspicions. In this context, it should be noted that legal measures have been taken to effectively combat bogus companies, primarily as a result of the Fraud Prevention Act, which came into force in 2024. Persons authorised to exercise the profession have to deal intensively with these new legal provisions, which leads to additional sensitisation in this area.

The insight gained from the analysis of criminal statistics and the A-FIU's suspicious activity reports that customs offences can be regular predicate offences to money laundering is of very minor relevance to the tax consultancy and auditing services sector. This is due to the fact that, in practice, tax advisors and auditors only exceptionally represent clients before the customs authorities or support them in the fulfilment of customs obligations.

In the area of terrorism financing, there is a risk that legal sources of financing or the use of funds for terrorist organisations and individuals, e.g. through donations (collections), earned income, social welfare, etc., will be used. are utilised. Due to the fact that there are large and active communities from relevant countries in Austria, which have lively associations as well as financial connections to their home countries, the risk of terrorism financing is generally classified as high. In the tax advisory and auditing services sector, it has not yet been observed that the activities of

tax advisors or auditors have been misused for terrorism financing purposes. This assessment is also confirmed by the close coordination of KSW with the A-FIU and the BVT and BMI on the occasion of the terrorist attack in Vienna in 2020.
The Austrian Chamber of Tax Consultants and Auditors (KSW) has no evidence that the professions are being abused on a large scale for money laundering and terrorism financing activities. The criminal prosecutions and convictions reported to the chamber on the basis of professional regulations do not show any proactive involvement of professionals in money laundering schemes. There are no known statistics to suggest otherwise.

Conclusion: Based on the summarised scenarios of the Supranational Risk Assessment, which suggest a significant threat, the current national data shows that no significant threat can be assumed in the tax advisory and auditing services sector based on the national data and statistics. To summarise, the threat can therefore be classified as low to medium.

Proliferation financing
As explained in the National Risk Assessment, weapons, military goods and dual-use goods are subject to authorisation in the area of export controls. The threat is that, contrary to official statements, weapons of mass destruction, delivery systems, dual-use goods and corresponding know-how could be exported and end up in the possession of sanctioned regimes or terrorist organisations or be misused for proliferation-relevant purposes. In the case of dual-use goods in particular, utilisation for military purposes cannot be ruled out. Closely linked to the phenomenon of proliferation is the phenomenon of money laundering and the risk of circumventing targeted financial sanctions.

In the case of "risk-prone" transactions, but also a certain proximity of sanctioned persons or companies and weapons, delivery systems and dual-use goods, circumvention transactions are potentially possible. However, the Chamber of Tax Consultants and Auditors in Austria has no indications that the services of tax consultants and auditors are used for proliferation financing purposes.

Conclusion: In summary, the threat that the services of tax advisors and auditors will be used for proliferation financing purposes can be classified as low.

Vulnerability

Money laundering and terrorism financing
As in the Supranational Risk Assessment, we would like to point out that the assessment of vulnerability to terrorism financing in connection with the services of auditors and tax advisors was examined together with money laundering. The vulnerability to terrorism financing therefore does not require a separate assessment. Proliferation financing and targeted financial sanctions have been added to the scope of preventive measures as a result of an amendment to the law. There is also no need for an assessment of vulnerability due to these.
In the summarised scenarios of the Supranational Risk Assessment, the vulnerability of services provided by tax advisors and auditors with regard to misuse for the purposes of money laundering

and terrorism financing was classified as significant. The national vulnerability will be derived below.

(a) Risk potential:

Risks exist primarily due to the services offered by the professional groups.

The risk of the respective "services being misused for laundering the proceeds of criminal activities" must be assessed (Recitals 14 and 16, 2nd ML). In the case of auditing activities (see below), there is no such risk of abuse at all and in the case of "tax advice" the risk is considered to be equally high for all service providers; only in the case of money laundering-related transactions is this risk higher than in the case of non-money laundering-related transactions. Insofar as the activities involve the mapping of business transactions that have already taken place in a legally defined form (preparation of accounting without involvement in these business transactions themselves), there is generally no increased risk of abuse for money laundering purposes.

Consequently, an overview of the most relevant services of the two professional groups and their risk potential will now be provided:

Payroll accounting:

These services range from determining employees' entitlements, calculating reimbursement of expenses, etc. to support and representation in wage tax, social security and municipal tax audits. In the context of payroll accounting, the risk of professional groups being misused for the purposes of money laundering and terrorism financing is considered to be low to medium. Unlawful behaviour, such as the circumvention of illegal employment, etc., can be recognised and reported by the person entitled to exercise the profession in part and with reference to article 77 para. 6 WTBG 2017.

Accounting

Accounting services include, among other things, keeping accounts on the basis of documents provided by the client, preparing and submitting advance VAT returns and providing monthly balance lists for real and personal accounts. Here too, the risk of the professional groups being misused for money laundering and terrorism financing purposes is considered to be low to medium. Persons entitled to exercise the profession may be able to identify anomalies and report any unlawful transactions. However, this can be made considerably more difficult by the submission of falsified receipts or transactions. At this point, reference can also be made to the comments on article 77 para. 6 WTBG 2017 set out at the beginning.

Preparation of annual financial statements

The annual preparation of the annual financial statements is one of the core activities for tax consultants and auditors. Persons entitled to exercise the profession are usually involved in all steps of the preparation of the annual financial statements. This is precisely where the indirect and retrospective "observer role" of persons entitled to exercise the profession mentioned above becomes clear. Although they are not directly involved in the financial and economic processes of the company, they gain a precise insight into the financial and economic processes of the company in the past financial year in the course of preparing the annual financial statements. Tax advisors and auditors are therefore able to recognise suspicious facts relating to money laundering and terrorist financing retrospectively. In this regard, they would be subject to a

reporting obligation to the Financial Intelligence Unit of the Federal Ministry of the Interior. However, the risk of the professional groups being misused for money laundering and terrorist financing purposes when preparing the annual financial statements is considered to be low to medium. This would only be possible through the active (prohibited) false preparation of annual financial statements by a tax consultant or auditor.

Consultancy (incl. tax returns and expert opinions)

Consultancy work is another focus of the services provided by tax consultants and auditors. These are primarily advisory services in the area of tax law and accounting, but also advice in connection with labour issues, in matters relating to contributions, insurance and benefits from social security institutions and in the area of restructuring advice. Other areas of advice are also mentioned in articles 2 and 3 of the WTBG 2017, which are also provided in individual cases. In most of these areas of advice, those authorised to practise the profession are also authorised to represent clients. For example, in tax and criminal tax proceedings. Expert opinions on complex tax law issues are also prepared in this context. Many of these advisory activities do not fall under money laundering-related activities for other professional groups that are considered obliged entities and carry out the same advisory activities.

Another main activity in this context is the preparation of regular tax returns for clients.

Here too, as already explained above with regard to the preparation of annual financial statements, the role of the persons entitled to exercise the profession is primarily that of an indirect "observer". They are not directly involved in the financial and economic transactions of clients, but may gain insight into their financial and economic transactions in the course of their activities. It is therefore possible for tax advisors and auditors to subsequently recognise suspicions of money laundering and terrorist financing. In this regard, they would be subject to an obligation to report to the BMI's Financial Intelligence Unit. However, the risk of these professional groups being misused for money laundering and terrorist financing purposes in the course of their advisory activities is considered to be low to medium.

Fiduciary activity

Tax consultants and auditors occasionally also act in a fiduciary capacity as part of their professional activities. This is usually a fiduciary activity in connection with the processing of a transaction or the holding of investments (the latter must be reported to the tax office and also disclosed in accordance with the WiEReG). As persons authorised to exercise the profession carry out financial transactions directly for their clients, the risk of persons authorised to exercise the profession being misused for money laundering and terrorist financing purposes is considered to be medium to high. However, it should be noted that financial transactions carried out in this way are only processed with the involvement of banks or financial institutions, which in turn are bound by strict measures to prevent money laundering and terrorist financing. In this respect, there is therefore a control by the tax advisor/auditor on the one hand and by the respective bank or financial institution on the other. Furthermore, fiduciary activities are only occasionally performed by tax advisors and auditors in Austria and represent a rather insignificant area in relation to other activities.

Examination services

Audit services (i.e. audits, in particular of historical financial information) include statutory and voluntary audits as well as other statutory audits and other audit engagements. Auditors are never involved in the execution of transactions. The risk of these activities being misused for

money laundering purposes is almost impossible. A low risk is therefore assumed here. Persons entitled to exercise the profession who carry out statutory audits are inspected as part of the regular quality assurance reviews of the audit oversight authority (see below) and checked for compliance with measures to prevent money laundering and terrorist financing.

Furthermore, the risk potential can be determined on the basis of geographical risk and client risk.

Geographical risk

Tax consultants and auditors mainly provide their services within Austria. Small law firms and law firms in rural areas in particular usually only serve clients from the surrounding region. In contrast, there are large law firms that also operate across borders. These are usually law firms that are part of an international network (e.g. "Big Four" companies). Cross-border activities are primarily focussed on clients in EU member states. The provision of services for clients from third countries is much rarer. Occasionally, clients from high-risk countries are also served.

Statistically, this results in the following geographical distribution of the supported clients:

- Around 96.3 % of sales are attributable to domestic clients
- Around 2.3 % of sales are attributable to clients from EU member states
- Around 1.4 % of sales are attributable to clients from non-EU member states.

KSW therefore categorises the geographical risk of services provided by tax advisors and auditors as low to medium. If clients from high-risk countries are served, those authorised to exercise the profession are obliged to apply increased customer due diligence as part of the measures to prevent money laundering and terrorism financing - see the information on risk-minimising measures.

Client risk

As previously mentioned, tax consultants and auditors work for a wide range of clients. These can range from individuals and one-man companies to large and complex companies and networks. Furthermore, some persons entitled to exercise the profession also work for public institutions, municipalities and churches.

The economic sectors of the clients are also broadly diversified as a result. They include (financial) service companies, trading companies as well as construction companies and the like.

For this reason, a medium risk must be assumed in the area of client risk. A concrete determination of the money laundering and terrorist financing risk of a principal usually requires a case-by-case assessment by the respective tax advisor/auditor as part of the mandatory risk assessment.

However, an increased risk is indicated for certain clients. This is the case, for example, if the client is a PEP or a family member of a PEP or a person close to a PEP. There is also a high risk if the client is on the list of bogus companies.

Certain sectors can also indicate a supposedly increased risk. These include, in particular, cash-intensive sectors (especially restaurants, hotels, brothels, gambling establishments, etc.), companies in the construction industry and property developers, as well as real estate trading and trading in high-value goods (especially precious metals, precious stones, jewellery, watches, works of art, antiques, motor vehicles, ships, motorboats, aircraft, machinery, etc.) and import/export companies.

However, there are also circumstances that indicate a low risk of money laundering and terrorism on the part of the client.
This applies in particular to public, listed companies that are subject to disclosure obligations that impose requirements to ensure appropriate transparency with regard to beneficial ownership. Furthermore, such a low risk is indicated for public administration and public-law institutions and companies.

(b) Risk awareness:
Tax advisors and auditors must always apply strict (professional) due diligence standards when providing their services and observe general professional ethics.
Services in the areas of tax consultancy and auditing are also usually geared towards long-term business relationships. This also creates a certain level of trust between the professionals and their clients. Tax consultants and auditors are therefore able to evaluate their clients' economic and financial processes and recognise potential risks. Occasionally, however, there are also shorter and one-off services, particularly in the area of consultancy work.
Furthermore, they are obliged by professional law in accordance with article 71 (3) WTBG 2017 to keep their professional knowledge up to date at all times. KSW always endeavours to keep its members trained and informed in the area of money laundering and terrorist financing. KSW does this itself by organising any information events and themed evenings and by sending out newsletters. In addition, persons authorised to exercise the profession can also obtain information from KSW in writing and by telephone with regard to the prevention of money laundering and terrorist financing. This raises risk awareness in the profession.
KSW also regularly submits requests for information to relevant authorities, such as the FIU, in order to obtain the latest findings in the areas of money laundering and terrorism financing. These findings are then shared with the professional groups.
Finally, persons entitled to exercise the profession are obliged to regularly train their employees on the topics of money laundering and terrorism financing. This training must be documented and is also audited by KSW.
As a result of these measures, it can be said that there is a high level of risk awareness in the profession with regard to money laundering and terrorism financing. This is also largely confirmed by the results of the Chamber's supervisory activities regarding compliance with professional customer due diligence to prevent the misuse of members of the profession for the purposes of money laundering and terrorism financing (see below).

(c) legal framework and supervision/governance:
When carrying out their activities, tax advisors and auditors must always comply with the professional regulations and measures for the prevention of money laundering and terrorism financing as well as proliferation financing, which are set out in articles 87 - 105 WTBG 2017. In addition to these legal provisions, persons authorised to exercise the profession are also subject to the Regulation of the Chamber of Tax Consultants and Auditors on the Directive on the Prevention of Money Laundering in the Exercise of the WT Professions (KSW-GWPRL 2017), which sets out further measures, instructions and specifications.
Pursuant to article 101 WTBG 2017, the KSW, as the representative body for tax consultants and auditors, is responsible for supervising compliance with measures to prevent money laundering

and terrorism financing. For this purpose, 1.5 full-time employees are employed at the chamber office itself, who are supported by the Committee for Money Laundering Prevention Supervision, consisting of 8 functionaries, and the 21 experts who carry out on-site inspections. In addition, supervision is supported by the quality assurance auditors, who are listed as recognised quality assurance auditors by the Auditor Oversight Authority (currently 141 entries), in reviewing the auditors (in the course of the ongoing legally obliged quality assurance audits).

Supervisory audits of KSW pursuant to article 102 WTBG 2017

KSW conducts regular supervisory audits of its members to monitor compliance with measures to prevent money laundering and terrorism financing. These are ad hoc audits that are carried out using a risk-based approach. In addition, in the event of a specific incident, KSW may also conduct an incident-related audit.

As already mentioned, the ad hoc audits are carried out on the basis of a risk-based approach. The specific persons entitled to exercise the profession to be audited are selected at random. The audits can be carried out in two different ways.

On the one hand, through an offsite audit, in which the assessment is carried out on the basis of internal documents and information provided by the person entitled to exercise the profession. On the other hand, by means of an inspection at the premises of the person entitled to exercise the profession, including a random inspection of their order documents. An inspection must be carried out by experts within the meaning of article 103 WTBG 2017. Such experts come from the profession of tax consultants and auditors and are selected from among the investigating commissioners pursuant to article 140 WTBG 2017 or the quality auditors pursuant to article 26 (5) APAG. An additional requirement is proof of relevant training in the prevention of money laundering and terrorism financing.

KSW publishes an annual report on its supervisory activities on the KSW website.

Inspections as part of the quality assurance inspection

Persons authorised to exercise the profession who are entered in the public register in accordance with article 52 APAG are exempt from the above-mentioned ad hoc audits by KSW. However, these persons entitled to exercise the profession are audited by the Auditor Oversight Authority (APAB) as part of its regular quality assurance audits. The review is mandatory and takes place every 3-6 years. In order to ensure a standardised procedure for the independent audits of the KSW and the APAB, the KSW has drawn up a statement on the procedure for the audits. In the event of problematic findings by the APAB, the APAB is also obliged to notify the KSW, as the KSW remains the sole supervisory authority for the prevention of money laundering and terrorism financing. Furthermore, the KSW is also free to carry out an event-driven audit of this person authorised to exercise the profession, provided there is of course a reason for suspicion.

<u>Conclusion</u>: Based on the summarised scenarios of the Supranational Risk Assessment, which suggest a significant vulnerability, the framework conditions presented mean that the vulnerability of tax advisors and auditors to being misused for the purposes of money laundering and terrorism financing can be classified as low to medium.

Risk minimisation measures

Risk-minimising measures by the persons entitled to exercise the profession

The risk minimisation measures of tax advisors and auditors are regulated in articles 89 - 100 WTBG 2017.

The following is a list of individual customer due diligences that apply to tax advisors and auditors.

Identification of the client

If the client is a natural person, identification must be provided by means of a current official photo ID. The same applies to the legal representatives of non-natural persons as clients (article 90 Z 3 WTBG 2017). If no current official photo ID is available for the identification of a natural person, article 1 para. 1 KSW-GWPRL stipulates that the verification can also be based on other sources on a risk-based basis. In this context, information and information from reliable guarantors is considered credible. These include courts and other state authorities, tax advisors, auditors and persons with comparable foreign professional authorisation, notaries, lawyers and credit institutions, provided they do not have their official sphere of activity, registered office or place of residence in a non-cooperating state within the meaning of article 94 (5) WTBG 2017.

If the client is a legal entity, persons entitled to exercise the profession must establish and verify the identity of the legal entity and the identity of the client's representative. In addition, the existence of a valid power of representation must be verified. The identity of beneficial owners must also be established, e.g. by questioning the client's legal representatives. The status as beneficial owner and the identity must be verified by taking risk-orientated and appropriate measures, e.g. by inspecting the commercial register or the beneficial ownership register (WiEReG). At the beginning of a new business relationship with a legal entity pursuant to article 1 WiEReG, persons authorised to exercise the profession must obtain an extract from the register of beneficial owners pursuant to article 9 or article 10 WiEReG as proof of registration of the beneficial owners (article 91 (4) WTBG 2017). The identification of the client includes appropriate measures for tax advisors and auditors to understand the ownership and control structure of the client. If there is only a low potential risk in an individual case that the services of the person authorised to exercise the profession will be misused for money laundering or terrorism financing purposes, it may be sufficient to obtain a general understanding of the ownership and control structure of the client by general means, even if there is no other indication of an increased risk.

In the case of other representatives, the principal must be identified in addition to the representative and both the identity of the representative and the valid authorisation to represent must be verified. Article 1 (3) KSW-GWPRL stipulates that a written power of attorney must be obtained for this purpose; only in the case of professional party representatives is it sufficient to refer to a power of attorney granted together with proof of professional authorisation.

PEP query

When entering into a new business relationship, tax advisors and auditors must determine whether their client is a PEP. Article 94 para. 1 no. 4 WTBG 2017 (Enhanced customer due diligence) clarifies that PEPs, their family members and persons known to be related parties must be treated equally from a risk perspective. This group of persons is defined in article 87 (2) Z 14 - 16 WTBG 2017. It is the responsibility of the profession to determine how to check whether a client or beneficial owner belongs to this group of persons. For the most part, this is carried out by means of queries in specialised databases to check persons in this regard, in particular with regard to their classification as politically exposed persons (PEP).

Law firm risk analysis

The person entitled to exercise the profession must classify all typical professional activities offered or carried out in his law firm into one of the risk categories high/medium/low according

to the risk of being misused for money laundering or terrorism financing purposes on the basis of the EU risk assessments, the national risk assessment and the risk factors in Annexes 1 - 3 of the 4th ML Directive.

Law firm guide

Pursuant to article 88 para. 3 WTBG, the person entitled to exercise the profession must summarise all strategies and methods used to fulfil the GWP obligations, as well as the internal documents and working papers used for this purpose and the documentation systems used, in a GWP law firm guide. This must be demonstrably brought to the attention of all employees.

The size and complexity of the law firm, the duration and type of service provided, the person of a client or beneficial owner, the client structure and the regions in which the person entitled to exercise the profession provides his or her services must be taken into account. The law firm guide must also contain information on the KSW whistleblower system and, depending on the size of the law firm, on the law firm's internal whistleblower system. It must also indicate the location where the currently applicable law firm guidelines can be viewed by employees and clarify who is responsible for answering questions. In addition, reference should be made to the right of inspection of the KSW or, if applicable, the auditor oversight authority in connection with the GWP audits.

Money Laundering Officer

Persons authorised to exercise the profession must set up a special officer for money laundering and terrorism financing issues if this is necessary due to the nature and scope of the business activity (article 99 para. 2 WTBG 2017) The person authorised to exercise the profession must ensure that the money laundering officer has sufficient professional qualifications, knowledge and experience at all times (professional qualifications) and is of integrity (personal reliability).

ML prevention documentation

Decisions on the content of order-related customer due diligence and their basis must be documented on a risk-based basis. Article 98 WTBG (documentation and retention obligations) standardises that persons authorised to exercise the profession are generally obliged to do so,

1. documents that serve to fulfil customer due diligence obligations towards clients,
2. receipts and records of transactions,
3. documents that have been submitted in connection with suspicious activity reports and
4. documents in connection with the client's risk classification,

five years after the last business transaction (or after the execution of the transaction in question). The period runs from the end of the calendar year to which the last business transaction relates.

Employee regulations

Pursuant to § 99 para. 1 no. 2 WTBG, persons authorised to exercise the profession must fulfil special obligations with regard to their staff:

Pursuant to article 99 para. 1 no. 2 lit a WTBG 2017, staff must be subject to a money laundering or terrorism financing check upon recruitment. Pursuant to article 99 para. 1 no. 2 lit b and c WTBG 2017, employees must be demonstrably familiarised with the law firm's internal regulations and trained in special training programmes. Completion of the training programme and the content of the training must be documented.

Risk profile

A risk profile must be drawn up for each order to assess the risk of money laundering or terrorism financing. The person entitled to exercise the profession must draw up a risk profile for each order on the basis of all information received about the client, the service and the law firm risk and the associated information and keep it up to date for the duration of the business relationship. With regard to the service risk, the assessment in the law firm risk analysis must be used.

The level of order-related risk identified in the risk profile also determines whether lower or higher customer due diligence requirements are to be applied. The frequency with which the documented data is regularly updated also depends on this risk categorisation. Data relating to an order with an increased risk must be updated more frequently than data relating to an order with a lower risk, even if there is no reason to do so. In the case of an order with an increased risk, the risk profile must be updated at least once a year.

Customer due diligence in the customer acceptance process

In the case of a natural person as the principal, identification must be provided by means of a current official photo ID. The same applies to the representative of a non-natural person as the principal (article 90 no. 1 WTBG - Scope of customer due diligence). A photo ID that expires in the course of the business relationship does not change the original identification. Suitable photo ID cards must be provided with a non-replaceable - i.e. to be attached by the authority - recognisable head image of the person to be identified, which does not obviously differ from the person identifying themselves personally.

If no current official photo ID is available for the identification of a natural person, article 1 para. 1 of the KSW-GWPRL (organisation of customer due diligence) stipulates that the verification can also be based on other sources on a risk basis. Information and information from reliable guarantors is considered credible. These include courts and other state authorities, tax advisors, auditors and persons with comparable foreign professional authorisation, notaries, lawyers and credit institutions, provided they do not have their official sphere of activity, registered office or place of residence in a non-cooperating state within the meaning of article 94 (5) WTBG (enhanced customer due diligence).

Audits of unusual transactions

Unusual transactions within the meaning of article 94 para. 1 no. 1 WTBG 2017 mean that persons authorised to exercise the profession must set the risk classification to high risk until clarification. They are also scrutinised to determine whether the origin and use of funds is legal. This must be done by appropriate means. An unresolved factual situation could expose the person authorised to exercise the profession to the risk of becoming a contributor to criminal money laundering as defined in article 165 of the Austrian Criminal Code (StGB) on the one hand, and not complying with the obligation to submit a suspicious activity report on the existence of funds from criminal activities in accordance with article 96 WTBG 2017 on the other.

Suspected cases

For a tax advisor or auditor to be obliged to report, it is sufficient that there is a suspicion that financial resources within the meaning of article 87 para. 2 no. 6 WTBG 2017 originate from criminal activities within the meaning of article 87 para. 2 no. 2 WTBG 2017 or are associated with terrorism financing, regardless of the amount involved. Persons authorised to exercise the profession must carry out a more detailed examination of the available evidence in the event of suspicion. Article 87 para. 2 no. 7 WTBG 2017 defines a reasonable suspicion as "the assumption of the probability of the existence of a certain fact based on knowledge of sufficient factual

indications. This assumption must go beyond a mere presumption." Accordingly, a suspicion exists if "sufficient factual indications justify the assumption of the probability of the existence of certain circumstances, whereby a suspicion is more than a mere presumption. A suspicion can only ever arise on the basis of conclusions drawn from facts - an offence can be inferred from knowledge of facts according to life experience." Finally, it should be noted that to the extent that it is assumed that the requirements for "reasonable grounds to suspect" are lower than those for suspicion, doubts are indicated because it is hardly recognisable to what extent suspicion - in view of the definition presented - sets higher requirements than the existence of reasonable grounds to suspect contact with incriminated property." (Brandl/Bülte, Die Geldwäsche-Verdachtsmeldepflicht und das Vertrauensverhältnis zwischen Berater und Mandant in Leitner/Brandl (eds.), Finanzstrafrecht 2019)

Obligation to report

If the person authorised to exercise the profession suspects that financial resources, regardless of the amount involved, originate from criminal activities or are associated with terrorism financing in the course of their professional activities, they must immediately inform the Financial Intelligence Unit of their own accord by means of a report (article 96 para. 1 WTBG 2017). Furthermore, they must consider submitting a suspicious activity report if they are unable to fulfil their customer due diligence obligations with regard to determining and verifying the identity of the client, the beneficial owner or the assessment and appropriate collection of information on the purpose and intended nature of the business relationship (article 96 para. 3 WTBG 2017).

In addition, pursuant to article 96 para. 2 WTBG 2017, they must provide the Financial Intelligence Unit directly or indirectly with all additional information immediately upon written request, provided that this does not conflict with procedural or professional law prohibitions or rights to refuse to testify. The reporting obligation and the general application of the provisions regarding the prevention of money laundering in articles 88 - 100 WTBG 2017 must be understood to refer exclusively to facts that arise in the course of the professional activity of the person authorised to exercise the profession.

Risk-minimising measures taken by KSW

In addition to the following risk-minimising measures, we refer to the comments under "(c) Legal framework and supervision/governance", which also qualify as risk-minimising measures of KSW.

Training in the area of money laundering prevention and terrorist financing by KSW

KSW always endeavours to train its members in the area of money laundering and terrorist financing and to keep them informed. KSW does this itself by organising information events and theme evenings and by sending out newsletters. In addition, persons authorised to exercise the profession can also obtain information from KSW in writing and by telephone with regard to the prevention of money laundering and terrorist financing. Tax consultants and auditors are also legally obliged to provide evidence of a specified level of further training. Most of this further training is completed at the Academy of Tax Consultants and Auditors (ASW), a wholly owned subsidiary of KSW. In recent years, the ASW has greatly expanded its range of training and further education courses focussing on the prevention of money laundering and terrorist financing. The ASW also acts as a training academy for prospective professionals. Candidates are therefore also increasingly trained in the prevention of money laundering and terrorist financing as part of their professional training. The ASW's money laundering prevention training app should also be

mentioned at this point. This training app is used by many professionals for further training and for training law firm employees and helps to sensitise both the profession and its employees.

The KSW whistleblower system pursuant to article 100 WTBG 2017

KSW has had a whistleblower system since 1 January 2019. This whistleblower system is accessible to everyone and is used to anonymously report persons authorised to exercise the profession who do not comply with the measures to prevent money laundering and terrorism financing set out in the WTBG 2017. Every report by a whistleblower is examined by KSW and may lead to the initiation of an investigation and disciplinary proceedings.

By May 2020, only one report had been made via the KSW whistleblower system. However, this report concerned the alleged money laundering activity of a client of a persons entitled to exercise the profession, which is why it was forwarded to the Financial Intelligence Unit of the Federal Ministry of the Interior as the FIU.

Total risk

The overall risk of the tax consultancy and auditing sectors is categorised **as low to medium**.

Recommendations

To improve the prevention of money laundering and terrorism financing, KSW would encourage a better and more comprehensive exchange of information between the authorities. There is already an ongoing exchange with the FIU, the Anti-Fraud Office and the WiEReG authority, but there should be an active forwarding of information from the Financial Intelligence Unit to KSW if persons authorised to exercise the profession are affected or processes are discovered that indicate an increase in the misuse of the services of tax advisors and auditors. Furthermore, the exchange of information with other authorities and institutions, such as the FMA, the OENB or financial institutions, should be intensified and further promoted.

13 Sectoral risk assessment of accounting professions

General description
With the entry into force of the Federal Act on the Accounting Professions (Accounting Act 2014 - Accountancy **Act 2014**; Federal Law Gazette I No. 191/2013) on 1 January 2014, the **President of the Austrian Federal Economic Chamber is responsible for enforcing the Accounting Act** as the **accounting authority**, i.e**. as a federal authority with delegated powers**. **The office of the Balance Sheet Accounting Authority** in the Austrian Federal Economic Chamber is responsible for **the operational exercise of** this responsibility. The accounting professions **are accountants, bookkeepers and payroll accountants** (article 1 Accountancy Act 2014). Only **natural persons who** have been **publicly appointed** and **companies that** have been **recognised** can exercise the powers within the scope of the respective authorisation (articles 2 - 6 Accountancy Act 2014): **Payroll accountant** Payroll accountants calculate employees' wage and salary entitlements and determine other components such as reimbursement of expenses, travelling expenses, etc. **Accountant** The accountant's scope of authorisation includes the pagatoric accounting (business accounting) including the preparation of balance lists for companies and the income and expenditure statement and imputed accounting. **Accountant** In addition to the above-mentioned areas of payroll accounting and bookkeeping, the scope of authorisation includes, in particular, the preparation of balance sheets, but only up to the characteristics specified for small corporations. Professionals in the accounting professions are typically not directly involved in the economic and financial processes of their clients and their transactions, but record them in the accounts after completion. **All active persons authorised to exercise the profession** must take **appropriate measures to prevent money laundering and terrorism financing** (articles 43 - 52d Accountancy Act 2014). The

level of measures to be taken by those authorised to exercise the profession has been specified by the accounting authority in the **2014 Accounting Professions - Practice Guidelines** (BB-AR 2014), including its 2018 amendment.

The accounting authority **is responsible for supervising compliance** (article 52f Accountancy Act 2014).

Threat

Terrorism financing

In the summarised scenarios of the Supranational Risk Assessment, the **threat** of **professional accountants** being misused for terrorist activities was classified as **high**. The **national threat** will be derived below.

In the accounting professions sector, the **picture is clear**: those authorised to work in the accounting professions **do not** come **into contact** with **threats in connection with terrorism financing**.

This picture emerges from the **current information (survey of 4,285 active professionals, as at 31 August 2024**) available to the Accountancy Act on the basis of the implementation of its supervisory duties (article 52f Accountancy Act 2014). This is probably primarily due to the **generally smaller business structures** (98% have no or fewer than 11 employees; 77% are sole traders; 90% have fewer than 100 clients), **typical client structures** and the **services typically provided** by the accounting professions.

For example, authorised accountants **do not** have **any conspicuous clients** from a terrorism financing perspective and are **completely familiar with their business practices**. This is partly due to the fact that authorised accountants **have** their clients **almost exclusively in their local area and have known them for a long time**.

No evidence was found that persons authorised to practise in the accounting professions are being abused for the purposes of terrorism financing.

This information is further confirmed by the fact that since 2020, only **one report** (as at 31 August 2024) has been made via the Internet-based whistleblowing system of the accounting authority (article 52e Accountancy Act 2014).

The Ministry of Labour and Economy (BMAW) and the Financial Intelligence Unit regularly provide the accounting authority with information (article 51i (2) Accountancy Act 2014).

Conclusio:

In contrast to the scenarios in the Supranational Risk Assessment, the current national data shows a completely different picture. To summarise, the threat to the accounting professions can be classified as low.

Money laundering

In the summarised scenarios of the Supranational Risk Assessment, the **threat** was classified as **high**. The **national threat** will be derived below.

The picture of the accounting professions sector with regard to money laundering is also very clear: **those authorised to practise** in the accounting professions **rarely come into contact with a threat in connection with money laundering**.

Due to the **smaller business structures** of those authorised to exercise the profession, there appears to be a **fundamental reluctance** to **accept individual clients with a potentially high money laundering risk** or **great caution when accepting** such clients, for fear of high administrative costs and/or sanctions or consequences associated with such clients. The **typical client structure** mentioned above, consisting of clients who **come almost exclusively from the local area and have been known for a long time**, should also be mentioned in this context.

Based on current information (as at 31/08/2024), 73% of those entitled to exercise the profession have customers with cash-intensive transactions (e.g. construction industry, retail).

Typically, those authorised to practise in the accounting professions are not involved in real estate transactions and transactions involving luxury goods.

84% of those entitled to exercise the profession are aware of the list of bogus companies published by the Federal Ministry of Finance.

Only 2% of persons entitled to exercise the profession have politically exposed persons (PEPs) as clients.

Less than 1% have customers in the areas of virtual currencies and cryptoassets.

Qualified accountants are not usually involved in transactions, but only record them in the accounts once they have been concluded.

In summary, those authorised to practise in the accounting professions do not typically work in areas with a high threat potential.

The **geographical distribution of the clients** of the accounting professions is clearly shown by the current information (as at 31 August 2024) available to the accounting authority on the basis of the performance of its supervisory duties (article 52f Accountancy Act 2014). The clients of the accounting professions are

- 89% Austrian clients with their sole main residence in Austria
- 9.44% clients from the EU
    - with a clear link to the CEE region or neighbouring member states
    - with the strongest connection to Austria
- 1.56% clients from non-EU countries
    - with a clear link to the CEE region: in particular Serbia, Bosnia and Turkey
    - with a relevant connection to China and the USA
- 99.77% of clients from low-risk countries
- 0.23% clients from high-risk countries

No evidence was found that members of the accounting profession are being misused for money laundering purposes.

This information is further confirmed by the fact that since 2020, only **one report** (as at 31 August 2024) has been made via the Internet-based whistleblowing system of the accounting authority (article 52e Accountancy Act 2014).

The BMAW and the Financial Intelligence Unit regularly provide the accounting authority with information (article 51i (2) Accountancy Act 2014).

Conclusio:
In contrast to the scenarios in the Supranational Risk Assessment, the current national data shows a completely different picture. To summarise, the threat to the accounting professions can be classified as low.

Proliferation financing

With regard to proliferation financing, a clear picture emerges in the accounting professions sector: **those authorised to practise** in the accounting professions **do not** come **into contact with a threat in connection with proliferation financing**.

As mentioned above, this is due to the **generally smaller business structures** of those authorised to practise the profession, the **typical client structure** and the **services typically provided**.

This is also confirmed by the above-mentioned current information (as at 31 August 2024) on the **geographical distribution of clients**.

No evidence was found that persons authorised to practise in the accounting professions are being misused for the purposes of proliferation financing.

This information is further confirmed by the fact that since 2020, only **one report** (as at 31 August 2024) has been made via the internet-based whistleblowing system of the accounting authority (article 52e Accountancy Act 2014).

The BMAW and the Financial Intelligence Unit regularly provide the accounting authority with information (article 51i (2) Accountancy Act 2014).

Conclusio:
To summarise, the threat can be classified as low.

Vulnerability

Terrorism financing
In the summarised scenarios of the Supranational Risk Assessment, the **vulnerability** of **members of the accounting professions** with regard to abuse for the purposes of terrorism financing was classified as **high**. The **national vulnerability** will be derived below.

(a) Risk potential:
As described above, the picture of the accounting professions sector from a terrorism financing perspective is **completely clear**: **those authorised to practise** in the accounting professions **do not** come into **contact with threats related to terrorism financing**.
The accounting professions sector **does not** appear to be **attractive for terrorism financing due to the services typically provided by those authorised to do so.**

(b) Risk awareness:
There is a high level of risk awareness among all those authorised to practise in the accounting professions. Services in the accounting professions are usually based on a **long-term business relationship**. This creates a certain level of **trust** between authorised accountants and their clients. Persons authorised to exercise the profession are obliged to keep their **professional knowledge up to date** and - if available - **to train** their **employees in the area of money laundering and terrorism financing**. This also raises risk awareness.

(c) legal framework and supervision/governance:
Persons authorised to practise in the accounting professions are **obliged to take measures to prevent money laundering and terrorism financing**.
and **comply with** their **obligations** in this regard (articles 43 - 52d Accountancy Act 2014). The accounting authority has specified the measures to be taken by those authorised to exercise the profession in the 2014 Accounting Professions - Practice Guidelines (BB-AR 2014), including its 2018 amendment.
Violations of professional **obligations in relation to money laundering/terrorism financing prevention are punishable by law.** (articles 52j - 52k Accountancy Act 2014).

The accounting authority, which is responsible for supervising compliance with the provisions relating to the
Money Laundering/Terrorism Financing Prevention, has prepared a **standardised risk assessment** (including explanations and definitions) for the survey of professionals carried out last year (see homepage of the accounting authority at

https://www.wko.at/bilanzbuchhaltungsbehoerde/verhinderung-der-geldwaesche-terrorismusfinanzierung). This risk assessment is intended to support those authorised to exercise the profession in fulfilling their professional obligations in relation to money laundering/terrorism financing prevention and can also be used by the authority as a **basis for an incident-related and incident-independent audit** (articles 52g ff Accountancy Act 2014).

Human and financial resources:

The accounting office has one **full-time employee available** for support the area of money laundering/terrorism financing prevention.

Conclusio:

Based on the summarised scenarios of the Supranational Risk Assessment, which suggest a high vulnerability, the framework conditions presented mean that the vulnerability of accounting professions to being misused for the purposes of terrorism financing is to be classified as low risk.

Money laundering

In the summarised scenarios of the Supranational Risk Assessment, the **vulnerability** of **persons entitled to exercise the accounting profession with** regard to abuse for the purposes of money laundering was classified as **high**. The **national vulnerability** will be derived below.

(a) Risk potential:

As described above, the picture of the accounting professions sector from a money laundering perspective is **very clear**: **those authorised to practise** in the accounting professions **rarely** come **into contact with a threat in connection with money laundering**.

There is **a low level of** vulnerability **from a geographical perspective**: The fact that the typical client structure consists almost exclusively of Austrian or geographical low-risk clients from the immediate vicinity means that **there is an increased sensitivity towards clients that do not fall into this typical pattern**.

There is also a **low level of** vulnerability **from the perspective of the activities of the products, services, transactions and/or distribution channels offered by the clients**.

Vulnerability **from the perspective of the client's activities**, on the other hand, exists **to a small but relevant extent** with regard to the **cash-intensive processing** of the client's activities. This aspect is partly due to the client structure of the accounting professions, which is largely characterised by the catering, retail and trade sectors.

(b) Risk awareness:

There is a high level of risk awareness among all those authorised to practise in the accounting professions. Services in the accounting professions are usually based on a **long-term business relationship**. This creates a certain level of **trust** between authorised accountants and their

clients. Persons authorised to exercise the profession are obliged to keep their **professional knowledge up to date** and - if available - **to train** their **employees in the area of money laundering and terrorism financing**. This also raises risk awareness.

(c) legal framework and supervision/governance:
Persons authorised to practise in the accounting professions are **obliged to take measures to prevent money laundering and terrorism financing**.
and **comply with** their **obligations** in this regard (articles 43 - 52d Accountancy Act 2014). The accounting authority has specified the measures to be taken by those authorised to exercise the profession in the 2014 Accounting Professions - Practice Guidelines (BB-AR 2014), including its 2018 amendment.
Violations of professional **obligations in relation to money laundering/terrorism financing prevention are punishable by law.** (articles 52j - 52k Accountancy Act 2014).

The accounting authority, which is responsible for supervising compliance with the provisions relating to the
Money Laundering/Terrorism Financing Prevention, has prepared a **standardised risk assessment** (including explanations and definitions) for the survey of professionals carried out last year (see homepage of the accounting authority at
https://www.wko.at/bilanzbuchhaltungsbehoerde/verhinderung-der-geldwaesche-terrorismusfinanzierung). This risk assessment is intended to support those authorised to exercise the profession in fulfilling their professional obligations in relation to money laundering/terrorism financing prevention and can also be used by the authority as the **basis for an incident-related and incident-independent audit** (articles 52g ff Accountancy Act 2014).

Human and financial resources:
The accounting office has one **full-time employee available** for support
the area of money laundering/terrorism financing prevention.

Conclusio:
Based on the summarised scenarios of the Supranational Risk Assessment, which suggest a high vulnerability, the framework conditions presented mean that the vulnerability of accounting professions to being misused for the purposes of money laundering should be classified as low risk.

Proliferation financing

(a) Risk potential:
As described above, the picture of the accounting professions sector from a proliferation finance perspective is **completely clear**: **those authorised to practise** in the accounting professions **do not** come into **contact with threats related to proliferation finance**. The accounting professions sector **does not** appear to be **attractive for proliferation financing** due **to the services typically provided by those authorised to practise.**

(b) Risk awareness:
There is a high level of risk awareness among all those authorised to practise in the accounting professions. Services in the accounting professions are usually based on a **long-term business relationship**. This creates a certain level of **trust** between authorised accountants and their clients. Persons authorised to exercise the profession are obliged to keep their **professional knowledge up to date** and - if available - **to train** their **employees in the area of money laundering and terrorism financing**. This also raises risk awareness.

(c) legal framework and supervision/governance:
Persons authorised to practise in the accounting professions are **obliged to take measures to prevent money laundering and terrorism financing**.
and **comply with** their **obligations** in this regard (articles 43 - 52d Accountancy Act 2014). The accounting authority has specified the measures to be taken by those authorised to exercise the profession in the 2014 Accounting Professions - Practice Guidelines (BB-AR 2014), including its 2018 amendment.
Violations of professional **obligations in relation to money laundering/terrorism financing prevention are punishable by law.** (articles 52j - 52k Accountancy Act 2014).

The accounting authority, which is responsible for supervising compliance with the provisions relating to the
Money Laundering/Terrorism Financing Prevention, has prepared a **standardised risk assessment** (including explanations and definitions) for the survey of professionals carried out last year (see homepage of the accounting authority at
https://www.wko.at/bilanzbuchhaltungsbehoerde/verhinderung-der-geldwaesche-terrorismusfinanzierung). This risk assessment is intended to support those authorised to exercise the profession in fulfilling their professional obligations in relation to money laundering/terrorism financing prevention and can also be used by the authority as the **basis for an event-driven and event-independent audit** (articles 52g ff Accountancy Act 2014).

Human and financial resources:
The accounting office has one **full-time employee available** for support
the area of money laundering/terrorism financing prevention.

Conclusion: In summary, the vulnerability can be classified as low.

Risk minimisation measures

Risk minimisation measures of the UBIT trade association
 	
• Provision of
  ○ Information (e.g. on goAML or PEP)
  ○ models (e.g. money laundering guidelines),
  ○ Checklists (e.g. for risk assessment or the identification of clients)

- PEP query option
- Training, lectures and webinars on the prevention of money laundering and terrorism financing

Risk minimisation measures by the supervisory authority

- Ongoing review of compliance with the obligations of those authorised to exercise the profession to prevent money laundering, terrorism financing and proliferation financing
- Ongoing sensitisation as part of the training obligation (article 33 (3) Accountancy Act 2014)
- Raising awareness as part of the implementation of supervisory duties, for example by providing a standardised risk assessment and case studies on its website (https://www.wko.at/bilanzbuchhaltungsbehoerde/verhinderung-der-geldwaesche-terrorismusfinanzierung) as well as through regular presentations, webinars and newsletters
- Establishment of a whistleblower system for the anonymous reporting of breaches of the obligations to prevent money laundering and terrorism financing by persons authorised to practise in the accounting professions (articles 43-52d Accountancy Act 2014)
- The provision of information by the BMAW and the Financial Intelligence Unit (article 52i (2) Accountancy Act 2014)

Total risk

To summarise, the overall risk in the accounting professions sector can be classified as low.

Recommendations

- Further intensification of cooperation and exchange of information between stakeholders
- Continuation of training and further education programmes
- Continue to provide up-to-date information from the Financial Intelligence Unit on methods of money laundering, terrorism financing and proliferation financing

14 Sectoral risk assessment gambling

General description of the gambling sector
The current EU anti-money laundering framework defines gambling services as services where a stake of monetary value is wagered in games of chance, including those involving elements of skill, such as lotteries, casino games, poker games and betting transactions, provided at a physical location or by any means, remotely, by electronic means or other communication technologies and at the individual request of a recipient of the service. The term "gambling services" therefore refers to a number of different services and distribution channels. For the purposes of this risk assessment, gambling services were subdivided according to the individual licences and authorisations provided for in the gambling sector, namely casino licences with live games and slot machines, lottery licence with classic lotteries, VLTs and electronic lotteries (online gambling), state-licensed slot gambling and betting.
Market entry and Fit&Proper provisions
In Austria, entrepreneurial gambling and betting can only be organised with a licence in accordance with the Austrian Gambling Act or state law. Pursuant to article 3 GSpG, the right to operate gambling services is reserved to the federal government (gambling monopoly). The federal government can transfer this right and certain licences and authorisations are provided for in the GSpG. The gambling monopoly severely limits the number of licences, there are strict requirements (public limited company with a supervisory board, high share capital, solid and prudent shareholders, capable management and supervisory boards) and licences can only be acquired under precise and strictly regulated legal conditions and after an official review. The Austrian Gambling Act (GSpG) stipulates mandatory requirements for licence applicants. Compliance with these requirements is monitored by the tax authority on an ongoing basis. Applicants must have the legal form of a public limited company and have paid-up share capital of at least EUR 109 million (lotteries) or EUR 22 million (casinos), the legal origin of which must be proven in an appropriate manner. The applicant must provide evidence that the requirements have been met (e.g. by presenting the financial situation of the entity, including any annual financial statements and audit reports for the last three years, proof of beneficial ownership in accordance with the FM-GwG) to the extent that a plausibility check can be carried out on the lawful origin of the funds. Shareholdings in the licence holders and intended changes to these shareholdings must be reported and subsequently reviewed and authorised by the authorities.

Persons who hold an interest in a licence holder and have a controlling influence must fulfil requirements that are imposed in the interests of sound and prudent management of the casino and regulatory reliability;

The applicant for a licence must guarantee the integrity and good reputation of the natural and/or legal persons who are or were directly or indirectly involved as owners and/or managing directors of shareholders with more than 25% of the applicant company.

The federal government holds an indirect stake in the current licence holders and exercises its supervisory rights via its members on the Supervisory Board and via state commissioners who are delegated to the Supervisory Board.

In addition to the regulations on licences and licence holders, the Gambling Act allows the federal states to authorise certain games of chance with slot machines (article 5 GSpG) through exceptions to the gambling monopoly. Article 5 GSpG represents a minimum standard. In order for provincial licences to be issued, the provinces must also enact laws on provincial gambling with slot machines. When enacting the relevant provincial laws, the provinces must observe the minimum standards set out in article 5 GSpG but may also stipulate stricter provisions.

The respective state laws also provide for regulations and checks on applicants comparable to those in the GSpG. In practice, both applicants and holders of licences under article 5 of the Gambling Act are therefore subject to strict legal regulations, including the regular performance of official audits, in which, for example, strategies with regard to the prevention of money laundering, terrorism financing and the non-implementation and circumvention of targeted financial sanctions in connection with proliferation financing are also reviewed.

Betting licences can also be issued by the federal states; here too, as described above, a comprehensive review procedure is carried out.

All offer listed below will therefore be allowed exclusively on the basis of a strict tender or selection procedure.

Conclusion: In the SNRA's summarised scenarios, the threat of infiltration at state-owned gambling companies that are subject to a licensing procedure was classified as **a non-relevant risk**. There are also no indications of a different threat situation at national level, which is why the threat and, in particular, the vulnerability are classified as **not relevant**.

Gambling in casinos (casinos)

General information

Gambling in casinos are gambling services within the meaning of Directive (EU) 2015/849 (Art. 3 no. 14) that are offered in the form of terrestrial gambling (in a physical location, automated or in the form of live gambling). According to the Austrian definition in article 1 of the Austrian Gambling Act (GSpG), gambling services are games in which the outcome of the game depends exclusively or predominantly on chance. Gambling services are in

particular the games roulette, observation roulette, poker, blackjack, two aces, bingo, keno, baccarat and baccarat chemin de fer and their game variants (article 1 (2) GSpG).

The measures provided for in connection with the prevention of money laundering, terrorism financing and the non-implementation and circumvention of targeted financial sanctions in connection with proliferation financing are regulated nationwide in the Austrian Gambling Act (GSpG). The GSpG refers to certain standards of the Financial Markets Anti-Money Laundering Act (FM-GwG).

Pursuant to article 3 GSpG, the right to operate gambling services is reserved to the federal government (gambling monopoly). The federal government can transfer this right and certain licences and authorisations are provided for in the GSpG.

There are currently 12 casinos in Austria operated by a single licensed provider (licence pursuant to article 21 of the Austrian Gambling Act).

The procedure for offering games in a casino can be described as follows (in accordance with the statutory obligations):

All visitors to a casino are identified and registered upon entering the casino. Subsequently, opportunities to purchase play money (game chips or credit on the player card) in exchange for cash or card payment are provided on the casino premises. Bitcoins or other virtual currencies cannot be used to purchase play money. Exchange is only possible using the player or admission card assigned to the player. These game chips or the player card can then be used to participate in the various games on offer. The game chips can be exchanged at the cash desk against re-identification of the guest. Participation in games is also only possible with a player card and after successful identification.

Participation in the game is only permitted for the player's own account.

Threat

Terrorism financing:

In the SNRA's summarised scenarios, the threat of casinos being misused for terrorist activities was classified as a **non-relevant** risk.

At national level, there are no indications of a different threat situation regarding casinos, which is why the threat is classified as **not relevant**.

In Austria, legal sources are used for financing or the use of funds for terrorist organisations and individual, e.g. through donations (collections), earned income, social assistance, etc. Fundraising through criminal offences (robbery, theft, fraud, etc.) has not been identified to date. There are no findings that would indicate an extension of these scenarios to casinos.

Terrorist organisations primarily collect funds from their own community. The money is collected through intermediaries via unregulated crowdfunding platforms. In the case of well-organised groups, (cultural) associations are operated to cover the true purpose, whereby the cultural purpose of the association is placed in the foreground to the outside world. There are no findings that would indicate an extension of these scenarios to casinos.

Money is transferred to the target country by official financial service providers (MVTS) and, if this is not opportune or possible, e.g. if there is no bank connection, by unofficial agents (hawaladars). Terrorist organisations generally also use cash couriers. On the other hand, transfers are made via a third country or through a correspondent bank located in another country if there is no direct bank connection to the target country. There are no findings that would indicate an extension of these scenarios to casinos.

The fundamental threats mentioned are **not considered relevant** with regard to casinos.

Conclusio

In summary, the threat is classified as not relevant.

Money laundering:

In the SNRA's summarised scenarios, the threat was classified as a **very high** risk. The following risk scenarios are mentioned in particular:

- Infiltration of the casino by criminal organisations (at management level);
- Interaction between employees and guests;
- Use of straw people ("mules") to acquire play money;
- Exploitation of gambling processes for the legitimisation of incriminated assets (e.g. by simultaneously betting on "red" and "black" in roulette) and the subsequent obtaining of a winning confirmation ;[12]
- Transaction of assets between several locations by utilising internal depots;
- Granting access rights to custody accounts to third parties;

Additionally for poker:

- Interaction of guests

Subsequently, the national threat will be derived: Threats exist through unknown customer origin, multiple registrations by one person, use of cash, use of foreign currencies, multiple use of payment methods by several customers, gambling participation by politically exposed persons (PEP), gambling participation by persons listed on sanctions lists, misuse of deposits, circumvention of deposit limits, malversation by an employee (issuing of winning confirmations/cooperation between guest and dealer), conversion of cash, use of counterfeit money, interaction between customers/guests, failure to follow up on suspected money laundering.

The threat of infiltration or acquisition of a casino by a criminal organisation mentioned by the SNRA does not exist due to the legal situation described above (see above). All other risks mentioned are to be contained in particular through the proper application of legal requirements. The overall risk of these threats is therefore classified as **high**.

[12] The SNRA clearly states that casinos within the EU generally do not issue winning confirmations without prior verification and that gambling without a winning confirmation does not qualify as money laundering. Austria follows this practice seamlessly.

Conclusio:

Based on the summarised scenarios of the SNRA, which suggest a very high risk of the threat, the current national data show a high risk. In summary, the threat is classified as high.

Proliferation financing:

Based on the national data available, the threat of casinos being misused for proliferation financing is classified as **a non-relevant risk.** Irrespective of this, licence holders are obliged to monitor sanctions lists (including proliferation financing).

Vulnerability

Terrorism financing:

In the SNRA's summarised scenarios, the vulnerability of casinos with regard to abuse for the purposes of terrorism financing was classified as **not relevant**. National vulnerability is also considered **as not relevant**, especially as there are no police findings or other practical experiences that indicate the opposite.

Conclusio:

To summarise, the vulnerability of casinos to being misused for the purposes of terrorism financing is not relevant.

Money laundering:

In the SNRA's summarised scenarios, the vulnerability of casinos with regard to abuse for the purposes of money laundering was classified as **medium.** The national vulnerability is to be derived below:

(a) Risk potential:

There is a very high proportion of cash turnover and the possibility of converting cash into play money and vice versa. In addition, numerous individual transactions take place in casinos, which makes monitoring difficult, especially during ongoing gambling operations. The possibility of setting up player deposits also involves risks, even if the establishment of such deposits is also suitable for increasing the transparency of the assets used.

The risk associated with types of gambling that can be controlled through the acquisition of skills (poker) or the use of targeted gambling behaviour (roulette) is to be classified as higher than the risk associated with other gambling services (such as slot machines within the casino).

(b) Risk awareness:

The risk awareness of the federal licence holder can be classified as high due to regular audits by the Tax Authority Austria and the awareness-raising discussions that take place as part of these audits. Employees regularly take part in risk-based training measures to prevent

money laundering, terrorism financing and the non-implementation and circumvention of targeted financial sanctions in connection with proliferation.

In addition, casinos are required to comply with comprehensive risk-based due diligence and reporting obligations. Regardless of the expected stake, access to casinos is only permitted after presentation of an official photo ID and a corresponding check of the customer's identity. Participation in the game is only possible with a personalised player card. In addition, the risk of money laundering is countered by appropriate monitoring systems in the casinos and by targeted sensitisation of employees with regard to the identification of suspicious gambling behaviour and other patterns of behaviour.

(c) Legal framework and supervision/governance:

Article 31c GSpG in conjunction with FM-GwG stipulates comprehensive due diligence and reporting obligations for casino operators (in addition to determining the identity of visitors, in particular the origin of funds and the comparison of data with PEP and sanctions lists). The Tax Authority Austria are responsible for monitoring compliance with the statutory provisions. Risk-based supervisory activities are currently carried out several times a year in varying degrees of intensity (on-site and off-site).

Conclusio:

Based on the SNRA, which suggests a medium vulnerability, the framework conditions set out above mean that the vulnerability of casinos to being misused for money laundering purposes can be classified as medium.

Proliferation financing:

National vulnerability with regard to misuse for the purposes of proliferation financing is also classified as **not relevant.** Irrespective of this, the licence holders are obliged to carry out monitoring of sanctions lists (including proliferation financing).

Risk minimisation measures

Pursuant to article 31c GSpG in conjunction with FM-GwG, comprehensive customer due diligence obligations with regard to the prevention of money laundering include the obligation to prepare an internal risk assessment and the complete identification and verification of the identity of visitors, the origin of funds and the verification of the purpose/type of business relationship as well as their continuous monitoring and the provision of the documentation required by the Gambling Act.

Not least due to the requirements of the EU Money Laundering Directive, increased customer due diligence requirements have been included in national gambling legislation. In particular, this is accompanied by a more extensive obligation to carry out checks if changes of EUR 2,000 or more are made per casino visitor and gambling day. This measure reduces the risk of the uncontrolled use of high assets.

At the beginning of 2025, the Tax Authority Austria published a circular that sets out sector-specific requirements for the implementation of the legal requirements and thus creates a standardised nationwide framework for the implementation of risk-based supervisory activities.

Furthermore, the Gambling Act obliges the Federal Minister of Finance to provide casino operators with up-to-date information on methods or indications of money laundering and terrorism financing as well as the non-implementation and circumvention of targeted financial sanctions in connection with proliferation financing. The Tax Authority Austria office fulfils this requirement by holding regular awareness-raising meetings.

Suspicious activity reports from persons obliged to report are checked by the Financial Intelligence Unit with regard to the recognised reason for reporting. If there are grounds for suspicion regarding terrorism financing, these SARs are further processed by the Directorate for State Security and Intelligence. In addition to potential criminal prosecution, the processing and analysis of suspicious activity reports by the Financial Intelligence Unit and the Directorate for State Security and Intelligence is also a primary way of minimising risk.

The Federal Minister of Finance has also set up a whistleblower system for reporting violations of money laundering regulations. The whistleblower system is publicly accessible at https://www.bkms-system.net/cal. All employees as well as guests have the opportunity to report incidents relating to money laundering anonymously via an existing whistleblower system. This option is communicated to all those affected via internal and external information channels, for example via the company's internal intranet page, periodic newsletters to all employees and also via the company's website. Regular information about the possibility of using the whistleblowing system also serves to raise awareness.

Total risk

In summary, the risk can be categorised as **medium**.

Recommendations

Further intensification of cooperation between companies and authorities and prompt information in the event of suspicions of money laundering.

Classic lotteries, electronic lotteries (online gambling), electronic lotteries via video lottery terminals

General information

Lotteries are gambling services within the meaning of Art. 3 no. 14 of Directive (EU) 2015/849. Lotteries are provided as **classic lotteries**, **electronic lotteries via video lottery terminals** (access via centrally networked terminals at fixed, publicly accessible operating locations) and **electronic lotteries** (participation in the game directly by the player via electronic media and centralised decision on the outcome of the game **(online gambling)).** Currently, all forms of lotteries are operated by a **single provider** (licence pursuant to article 14 GSpG).

Threat
Terrorism financing: The SNRA concludes that the risk of abuse for terrorist activities in the areas of **traditional lotteries** and **electronic lotteries via video lottery terminals** is **not relevant.** With regard to **electronic lotteries (online gambling)**, the SNRA assumes that the risk of misuse for terrorist activities is generally considered to be very high. This assumption is based on the fact that it is to some extent possible to use virtual currencies to participate in online gambling in other member states. Reference is made to a few cases where cryptocurrencies have been used to finance terrorist groups. However, the SNRA points out that there is no evidence to date that terrorist groups have also misused online gambling for financing and that conventional forms of financing (such as cash) continue to predominate. A future potential for abuse is seen in insufficiently regulated gambling markets. Apart from the findings of the SNRA, no additional threat scenarios were identified at national level. **Conclusio:** **To summarise, the threat to the areas of classic lotteries and electronic lotteries via video lottery terminals is not considered relevant.** **On the other hand, the risk that electronic lotteries in the form of online gambling could in general be misused for the financing of terrorist purposes must be classified as very high based on the findings of the SNRA.**
Money laundering: In the SNRA's summarised scenarios, the threat in relation to classic lotteries was classified as medium risk, in relation to electronic lotteries via VLT as medium risk and in relation to electronic lotteries (online gambling) as high risk. The national threat will be derived below: No national threats can be identified with regard **to classic lotteries**. Classic lottery products (in particular lottery tickets and instant lotteries) are sold exclusively via contractual partners in Austria and in euros. Any winnings are determined in a public and notarised draw or, in the case of instant lotteries, determined in advance, thus ruling out the possibility of malversation by employees. Due to the anonymity of the winners, contact by criminals with the intention of acquiring and redeeming a winning ticket for money laundering purposes is also very unlikely. In principle, the chance of winning in the lottery sector is extremely low. Taking the "Lotto" game as an example, the odds of winning first place are 1 in 8,145,060. A Lotto bet costs EUR 1.50. The average stake per ticket is EUR 9.22 (Lotto, LottoPlus and Joker). The maximum possible stake on a betting slip per round is EUR 1,849.70 for Lotto with the 012 system if LottoPlus is also played. From a prize payout of EUR 1,000.10, the winner is also identified. The maximum stakes are relatively low and the chance of winning is also very low, which means that the risk of money laundering **is not relevant**. National threats in the area of **electronic lotteries via video lottery terminals (VLT):** The risks of multiple use of payment methods by several customers, marked money and counterfeit money are countered insofar as players are required to identify themselves with an official

photo ID before participating in the game as part of a mandatory registration process. Furthermore, participation in the game is only possible with a personalised player card and multiple registrations by the same person are therefore excluded. When credit is loaded onto the player card, the banknotes are checked by a banknote acceptor in order to rule out the supply of marked money or counterfeit money. Non-cash payments are processed exclusively by an employee who verifies the customer's identity, which is why it is not possible for several customers to use the same non-cash means of payment. The national threat is therefore classified as **low** risk.

National threats in the area of **electronic lotteries (online gambling)** are: Omission of face-to-face identification, multiple registrations by one person, multiple use of payment methods by several customers, misuse of player accounts, circumvention of deposit limits, participation in games by politically exposed persons (PEP), participation in games by persons listed on sanctions lists, interaction between customers in poker and failure to deal with suspicions of money laundering. A medium risk can therefore be assumed at national level.

Conclusio:

Based on the summarised scenarios of the SNRA, which suggest a medium threat, the current national data show a low risk overall. In summary, the threat can be categorised as low.

Proliferation financing:

Based on the national data available, the threat of lotteries being misused for proliferation financing is classified as **a non-relevant risk**. Irrespective of this, the licence holders are obliged to monitor sanctions lists (including proliferation financing).

Vulnerability

Terrorism financing:

In the SNRA's summarised scenarios, the vulnerability of **classic lotteries and electronic lotteries via video lottery terminals** with regard to abuse for the purposes of terrorism financing was classified as **not relevant**. National vulnerability is also considered **not relevant.**

With regard to electronic lotteries in the form of **online gambling**, the national circumstances that differ from the SNRA must be taken into account. In addition to the fact that only one national provider has a licence for this form of gambling and operates this licence under strict regulatory conditions, it is not possible to participate in online gambling using cryptocurrency in particular. As these factors are essential for the result of the classification in the SNRA and no additional threat scenarios could be identified at national level, this means that national vulnerability is also **not relevant** for the area of electronic lotteries in the form of online gambling.

Conclusio:

In summary, it can be assumed that there is no relevant vulnerability.

Money laundering:

In the SNRA's summarised scenarios, vulnerability with regard to abuse for the purposes of money laundering was classified as **medium** for classic lotteries, **medium** for electronic lotteries via video lottery terminals (VLT) and **high** for other electronic lotteries. The national vulnerability will be determined below:

(a) Risk potential:

In **traditional lotteries**, there is a risk of money laundering if a winning ticket is taken from the winner and subsequently redeemed. With regard to **electronic lotteries via VLT**, there is a risk due to cash sales or the deposit and redemption of cash via player cards. **Electronic lotteries** (online gambling) involve the risk of participation by means of false identity due to the lack of face-to-face identification as well as the risk of unknown origin of funds due to the possibility of placing bets using Paysafe cards and Euro receipts.

(b) Risk awareness:

The risk awareness of the federal licence holder can be classified as high due to regular audits by the Tax Authority Austria and the awareness-raising discussions that take place as part of these audits. Employees regularly take part in risk-based training measures to prevent money laundering, terrorism financing and the non-implementation and circumvention of targeted financial sanctions in connection with proliferation.

(c) Legal framework and supervision/governance:

The provisions of the Gambling Act provide for increased customer due diligence to prevent money laundering (e.g. for the transfer of cash to playing cards in VLT). In addition, due to the gambling terms and conditions for **electronic lotteries (online gambling)** approved by the gambling supervisory authority, a deposit limit of EUR 250/week (under 26 years of age) or EUR 400/week (aged 26 and over) or higher limits (if affordable and after a corresponding review procedure has been carried out) per registered player and week applies.

Conclusio:

Based on the summarised scenarios of the SNRA, which suggest a medium vulnerability, the framework conditions presented mean that the vulnerability of lotteries to being misused for the purposes of money laundering can be classified as low.

Proliferation financing:

National vulnerability with regard to misuse for the purposes of proliferation financing is also classified as **not relevant.** Irrespective of this, the licence holders are obliged to carry out monitoring of sanctions lists (including proliferation financing).

Risk minimisation measures
Pursuant to article 31c GSpG in conjunction with FM-GwG, the lottery licence holder is obliged to carry out comprehensive customer due diligence with regard to the prevention of money laundering. In order to define and implement early measures, the lottery license holder has appointed an independent money laundering officer and also operates a certified risk management and monitoring system for conspicuous gambling behaviour. As there is only one licence holder for lotteries, the risk-minimising measures are based on the licence holder's practice: **Classic lottery products** are sold exclusively in retail outlets (tobacco, tobacconists, petrol stations, post offices, etc.) and the average stake amounts to EUR 5.50. The risk of third parties purchasing and redeeming winning tickets in classic lotteries is countered by ensuring the anonymity of the winners. This makes it virtually impossible for criminals to contact the winner in order to purchase the winning ticket from them and then redeem it themselves. To prevent money laundering, (sales) employees are regularly trained. Winnings of EUR 1,000.10 or more are paid out in accordance with the gambling terms and conditions approved by the Gambling Supervisory Authority exclusively at specially designated big-win payout centres upon presentation of an official photo ID, and winners are periodically checked against the PEP database. Stake limits and prize limits apply to **electronic lotteries via VLT**: each game is limited to a maximum stake of EUR 10 and a maximum prize of EUR 10,000, which strongly reduces the likelihood of abuse for money laundering. Furthermore, participation in electronic lotteries via VLT is only possible with a personalised player card upon presentation of an official photo ID. In order to fulfil the legal obligations, the identity of every visitor is checked and verified before entering the VLT outlet. Every visit is recorded in the central guest database. All guests are categorised into risk categories. As part of the customer identification process for each guest, i.e. for all risk categories, the guest data is always automatically checked against the PEP ("Politically Exposed Person", also in relation to family members and persons known to be close associates) and sanctions lists (EU, UN, etc.) in order to determine whether the visitor is a politically exposed person or a sanctioned person on this list. The licence holder uses the Dow Jones "Risk & Compliance" database, which provides PEP and sanctions lists for this purpose. If less than 5% of the amount booked on the player cards has been played at the VLT, the gambling system automatically generates a money laundering ticket (ML ticket) when cashing out. When paying out at the cash desk, an ML warning appears on the display. With regard to **electronic lotteries (online gambling),** there are increased requirements for registration: Participation in the game is only possible after the personal data has been recorded and can only be completed if it can be clearly proven by a combined check of first and last name and date of birth via a CRIF verification query or the ZMR (Central Register of Residents) that the player is not under 18 years of age and is resident in Austria. It is therefore not possible to participate in the game if you are resident in a third country. In addition, checks are carried out to determine whether the player (including family members and persons known to be close associates) is a PEP and/or is on a sanctions list (EU, UN, etc.).

The player must also set a limit for the maximum deposit amount per week at the latest when making the first deposit. Stakes are limited to a maximum of EUR 250.00/week (under 26 years of age) or EUR 400.00/week (over 26 years of age) per registered player and week for all payment methods. The maximum monthly limit is therefore generally EUR 1,600, which means that the risk of abuse for money laundering is **not relevant.** Higher limits (only possible for players aged 26 and over) must be requested separately and the necessary checks must be carried out by the licence holder's employees and documents must be provided to verify the origin of the funds and identity. Bitcoins or other virtual currencies cannot be used for the deposit.

Payouts from the electronic gambling balance are made exclusively by bank transfer to the player's bank account held in the EEA. Every payout of EUR 100 or more is subject to a plausibility check and must be authorised manually by the employees responsible for this. The bank account details must be disclosed at the time of the first withdrawal request. If the player has not yet undergone an extended identification process at this point in time, this must take place immediately before the first payout request. Pursuant to article 6 (4) FM-GwG, the following identification procedures are offered for this purpose: Online verification using the ID Austria full version, online verification using the photo ID chip procedure, online verification using the video ID procedure. A payout without extended identification is therefore not possible and multiple registrations of individual players are also prevented using this method. Furthermore, there will be a gradual switch to exclusive registration using ID-Austria exclusively.

Each player is continuously checked by a programme in the background and classified in risk classes (traffic light system), to which appropriate measures are linked.

Suspicious activity reports from obliged entities are checked by the Financial Intelligence Unit with regard to the recognised reason for reporting. If there are grounds for suspicion regarding terrorism financing, these SARs are further processed by the Directorate of State Security and Intelligence. The processing and analysis of SARs by the Financial Intelligence Unit and the Directorate for State Security and Intelligence is a primary way of minimising risk in addition to potential criminal prosecution.

Total risk

The overall risk can be categorised as **low**.

Recommendations

Further intensification of cooperation between companies and authorities and prompt information in the event of suspicions of money laundering.

Provincial games of chance with slot machines

General information

Provincial gambling services with slot machines are gambling services within the meaning of Art. 3 no. 14 of Directive (EU) 2015/849 in the form of terrestrial gambling conducted exclusively with slot machines (offline) at a physical location. Provincial games of chance with slot machines are games of chance with slot machines - subject to a type approval procedure and electronically connected to a central control system of the supreme gambling authority - in which the decision on the outcome of the game is made by a mechanical or electronic device in the machine itself, with limited stakes (max. EUR 10.00) and winnings (max. EUR 10.000, no jackpots) at fixed, publicly accessible operating locations (salons with a minimum of 10 and a maximum of 50 slot machines or a maximum of three slot machines in individual installations), in which no other gambling services may be offered (no live gambling), which are subject to official supervision in order to comply with the regulatory requirements placed on them, with special accompanying measures to prevent gambling addiction as well as money laundering and terrorism financing.

Provincial gambling with slot machines is regulated by state laws based on the provisions of the Austrian Gambling Act (GSpG) and the FM-GwG and is subject to licences. There are currently five so-called "licencing states" in Austria: Burgenland, Lower Austria, Upper Austria, Carinthia and Styria. In all other federal states, state gambling with slot machines is prohibited. There are currently six licenced companies in Austria that offer their gambling services with slot machines in the federal states.

Threat

Terrorism financing:

In the SNRA's summarised scenarios, the threat of slot machine gambling being misused for terrorist activities was classified as a **non-relevant** risk. The national threat is to be derived below:

In this respect, there is no real possibility of terrorism financing, as it is not possible to participate online, place bets or pay out winnings via electronic payment transactions. Disguised payments to terrorists therefore do not take place. Pre-determined profit distribution quotas prevent an increase in the funds used in the sense of financing.

Conclusio:

Based on the summarised scenarios of the SNRA, which suggest a non-relevant threat, the current national data shows that the financing of terrorist activities through national gambling with slot machines does not appear to be realistic and any residual risk is not relevant. To summarise, the threat is classified as not relevant.

Money laundering:

In the summarised scenarios of the SNRA, the threat was classified as a **medium** risk. The national threat will be derived below: Due to the **small amounts** that can be wagered (maximum EUR 10 per game) and won (maximum EUR 10,000 per game, no jackpots) in this form of slot machine gambling, it involves a **low** money laundering risk. In addition, all games played (as well as every stake and win) are recorded electronically and transmitted to the

central control system. Furthermore, participation in games is only possible with a **personalised player card** upon presentation of an official photo ID.

Conclusio:

Based on the summarised scenarios of the SNRA, which suggest a medium threat, the current national data show a low risk.

Vulnerability

Terrorism financing:

In the SNRA's summarised scenarios, the vulnerability of slot machine gambling with regard to abuse for the purposes of terrorism financing was classified as **not relevant**. The national vulnerability of machine gambling is also classified as **not relevant**.

Conclusio:

In summary, the vulnerability of slot machine gambling for terrorism financing purposes is not relevant.

Money laundering:

In the SNRA's summarised scenarios, the vulnerability of slot machine gambling with regard to abuse for money laundering purposes was classified as **medium.** The national vulnerability is to be derived below:

(a) Risk potential:

Slot machine gambling is primarily based on cash transactions. At best, money laundering could be carried out by charging a large amount of cash to the player card in order to then play with a small part of this amount and have the remainder paid out in cash.

(b) Risk awareness:

Risk awareness in the area of state gambling with slot machines can be categorised as high overall. In recent years, numerous information, exchange and training events have taken place to sustainably increase awareness within the sector. In addition, all gambling operators are required to sensitise their employees with regard to recognising suspicious transactions and patterns of behaviour.

(c) Legal framework and supervision/governance:

The relevant state laws provide for comprehensive due diligence and reporting obligations for gambling operators with regard to money laundering. In addition to establishing the identity of visitors, the origin of the funds and the comparison of the data with PEP and sanctions lists as well as the mandatory check as to whether visitors can be associated with a high-risk third country must be carried out.

The respective provincial government office is responsible for the supervision of provincial gambling licences. In order to improve the quality of risk-based supervisory activities, a private-public partnership initiative was carried out in 2022 under the auspices of the A-FIU, leading to a harmonised understanding of the partially divergent legal provisions and the

introduction of a nationwide risk-based audit approach. The results of this initiative are part of Austria's national strategy for the prevention of money laundering and terrorism financing.

Conclusio:

Based on the summarised scenarios of the SNRA, which suggest a medium vulnerability, the framework conditions described and in particular the possibility of only placing small amounts mean that the vulnerability of slot machine gambling to being misused for the purposes of money laundering can be classified as low.

Risk minimisation measures

Article 5 para. 6 GSpG provides for analogous compliance with the requirements for casinos and lotteries with regard to money laundering and terrorism financing for provincial lotteries with slot machines. The identity of visitors is recorded in accordance with article 31c para. 3 no. 1 GSpG using an official photo ID that fulfils the requirements of article 6 para. 2 no. 1 FM-GwG. The data of the official photo ID is recorded by means of scans or by manual entry. In addition, participation in a game is only possible with a personalised player card.

In order to counter the risk associated with cash wagers, depending on the federal state, information on the origin of the funds wagered must be obtained and verified when changing cash into gambling credits or vice versa and for accumulated wagers of EUR 2,000 or more. This obligation applies to accumulated stakes placed on one gambling day or in several apparently related transactions. The maximum possible stake is reduced to EUR 10 per game.

Total risk

The overall risk can be categorised as **low**, as slot machines tend to be unsuitable for money laundering.

Recommendations

Further intensification of cooperation between companies and authorities and prompt information in the event of suspicions of money laundering.

Betting

General information

Betting is a gambling service within the meaning of Art. 3 no. 14 of Directive (EU) 2015/849 and is offered on the basis of authorisations issued in accordance with the respective provincial legislation on bookmakers and totalisers. The competence for legislation and enforcement in the area of betting lies with the individual federal states. The requirements for the prevention of money laundering and terrorism financing as well as the non-implementation and circumvention of targeted financial sanctions in connection with proliferation financing vary from province to province but are based on the provisions of the FM-GwG.

Threat
Terrorism financing: In the SNRA's summarised scenarios, the threat of betting being misused for terrorist activities was classified as a **non-relevant** risk. The national threat is also classified as **not relevant.** **Conclusio:** **In summary, the threat is classified as not relevant.**
Money laundering: In the summarised scenarios of the SNRA, the threat was classified as **high** risk. The national threat will be derived below: Threats exist from infiltration of the business area by criminal organisations, match-fixing/betting fraud, purchase of winning tickets, calculated betting behaviour and anonymous betting or customers without identification. Overall, a **medium** risk can be assumed. **Conclusio:** **Based on the summarised scenarios of the SNRA, which suggest a high threat, the national data shows a medium risk. To summarise, the threat is classified as medium**.
Vulnerability
Terrorism financing: In the summarised scenarios of the SNRA, the vulnerability of betting with regard to abuse for the purposes of terrorism financing was classified as **not relevant.** National vulnerability is also classified as **not relevant**. **Conclusio:** **To summarise, the vulnerability of betting to being misused for the purposes of terrorism financing should be classified as not relevant.**
Money laundering: In the SNRA's summarised scenarios, the vulnerability of betting with regard to abuse for the purposes of money laundering was classified as **high**. The national vulnerability is to be derived below. **(a) Risk potential:** The greatest, nationally specific, risk is due to the high volume of bets, some of which are placed anonymously or without identifying the customer and using cash. Infiltration of the business operations by criminal organisations is considered unlikely due to the necessary authorisation procedures. **(b) Risk awareness:** The regulators and betting companies concerned are aware of the risk described above and are endeavouring to counteract it through appropriate legislation and internal company

measures. In recent years, a training initiative was organised by the Austrian Sports Betting Association with the aim of making every betting company in Austria aware of the risks associated with money laundering and terrorism financing. In addition, information, exchange and training events were organised by the authorities in order to sustainably increase awareness within the sector.

(c) Legal framework and supervision/governance:

In addition to detailed provincial legislation on combating money laundering, betting limits apply in 7 out of 9 federal states, with betting limits of between EUR 50 and EUR 70 in 5 federal states and EUR 500 and EUR 1,000 in two other federal states. Money laundering of large amounts would therefore require a large number of bets to be placed at different locations, which would be very costly and require a high degree of planning. In order to prevent money laundering, the betting behaviour of customers is also systematically monitored by means of internal risk monitoring and risk management.

The respective provincial government office is responsible for the supervision of betting providers. In order to increase the quality of risk-based supervisory activities, a private-public partnership initiative was carried out in 2022 under the auspices of the A-FIU, leading to a standardised understanding of the legal provisions, some of which differ from one another, and the introduction of a nationwide risk-based audit approach. The results of this initiative are part of Austria's national strategy for the prevention of money laundering and terrorism financing.

Conclusio:

Based on the summarised scenarios of the SNRA, which suggest a high vulnerability, the framework conditions presented mean that the vulnerability of betting to being misused for the purposes of money laundering is to be classified as medium.

Risk minimisation measures

The respective national laws provide for detailed measures to combat money laundering. IT-supported monitoring systems are used to recognise suspicious bets or transactions. In addition, the stakes are limited in the majority of federal states.

Total risk

The overall risk is categorised as **medium**.

Recommendations

Further intensification of cooperation between companies and authorities and prompt information in the event of suspicions of money laundering.

Appendix

General

Allocated human and financial resources pursuant to article 3 para. 3 no. 7 FM-GwG for the gambling sector

Regional authority	Human resources (FTE)*	Financial resources*
Federal Government	3	Financing from the overall budget
Burgenland	0,10	
Carinthia	1	
Lower Austria	0,14	
Upper Austria	0,50	
Salzburg	0,30	
Styria	0,30	
Tyrol	0,85	
Vorarlberg	2,5	
Vienna	0,40	

* These are figures from the Federal Ministry of Finance and the competent offices of the Federal State governments, which are largely based on estimates due to a lack of exact quantifiability.

15 Sectoral risk assessment for tradespersons

15.1 Insurance intermediaries

General description
The sector is a regulated industry under Art. 94(76) Trade Act 1994 and its inclusion in the obligations to combat ML/TF/PF is provided for in Art. 365m1(2)(4) Trade Act 1994. The enforcement reports of the trade authorities for 2023 assumed that around 12,500 companies fell within the scope of the provisions. However, the actual scope of application covers a much smaller number of companies. A comprehensive risk survey is currently carried out every two years at company level and, based on this, aggregated at geographical and sector level. The results of the risk survey include the risks from the SNRA and the NRA. There is also input from a criminological and typological perspective from the competent authorities and the FIU.
Threat
Terrorism financing In the summarised scenarios of the Supranational Risk Assessment, the threat of insurance intermediaries being misused for terrorist activities was classified as moderately significant (level 2). The national threat will be derived below. Threats exist in particular in the relatively high proportion of long-distance business where the customer was not present in person. In terms of the product, capital-forming insurance policies could probably be used primarily to transfer funds from one person to another, in that the contract holder and the beneficiary could be different people. This could be used to finance terrorist activities, especially if funds are transferred across borders. **Conclusion: In summary, the threat is classified as medium (2).**
Money laundering In the summarised scenarios of the Supranational Risk Assessment, the threat was classified as moderately significant (2). The national threat will be derived below.

Threats exist in particular due to the relatively high proportion of long-distance business where the customer was not present in person.

No particular current scenarios regarding the misuse of the sector for terrorism financing have been identified to date. In terms of the product, capital-forming insurance policies could probably be used primarily to transfer funds from one person to another, in that the contract holder and the beneficiary could be different people. This could be used to finance terrorist activities, especially if funds are transferred across borders.

Conclusion: In summary, the threat is classified as medium (2).

Proliferation financing

Threats exist in connection with proliferation financing in the form that weapons of mass destruction, delivery systems, dual-use goods and corresponding know-how come into the possession of sanctioned regimes or terrorist organisations, or that certain goods are misused for proliferation-relevant purposes contrary to official statements, represents one of the main proliferation-related threats. In this context, Austria is not only a transit country for proliferation-relevant goods, but also a destination country for illegal procurement activities due to its highly developed industrial production and the large number of small and medium-sized enterprises, which are world leaders in some areas. Dual-use goods, i.e. materials or products that can be used in both the civilian and military sectors due to their high level of development, pose a particular problem. Regulation EU 2017/1509 contains a basic regulation with regard to the People's Republic of Korea.

Insurance products are mainly used to cover any lack of pension benefits in old age and are less suitable for providing capital for proliferation financing. For this reason, no higher risk is generally to be assumed in connection with insurance intermediaries with regard to proliferation financing.

No threat scenarios or trends have been observed or reported in the recent past.

Conclusion: In summary, the threat is classified as low (1).

Vulnerability

Terrorism financing

In the summarised scenarios of the Supranational Risk Assessment, the vulnerability of insurance intermediaries with regard to abuse for the purposes of terrorism financing was classified as low/medium significant (1-2). The national vulnerability will be derived below.

(a) Risk potential:

The risk potential is considered to be relatively limited due to the relatively strong overall regulation of the sector. In principle, however, life insurance products and investment products

could lend themselves to terrorism financing, e.g. if foreign persons are beneficiaries of such insurance policies and funds could thus be transferred across borders.

(b) Risk awareness:
The fight against money laundering is the subject of training and further education for insurance intermediaries. Recently, as part of a two-year consultancy project (until September 2025) with an external consultant, various information events and awareness raising workshops have been held throughout Austria (as at October 2024, 8 to date by the BMAW with around 300 participants so far; others have been organised by other bodies, such as the FIU together with the Chamber), so it can be assumed that risk awareness has increased.

By continuing the far-reaching survey measures already mentioned and implemented in 2021, a further increase in risk awareness can be assumed and this is actually confirmed by the feedback from the trade authorities.

(c) legal framework and supervision/governance:
As part of the project with an external consultant, the legal framework and overall supervision in the commercial sector were comprehensively analysed. A corresponding action plan was created from the identified potential for improvement, the implementation of which will make it possible to improve the framework conditions and supervision.

Human and financial resources:
Equipping the authorities in terms of human resources and expertise was identified as a particularly important issue. With regard to the allocation of resources in this area, clear requests were made to those responsible in the federal states with organisational responsibility to increase the allocation of existing personnel resources to the area of AML/FT/PF. As far as can be seen from the feedback from the federal states, there has been an increase from 11 FTEs to 16 FTEs. With regard to the authorities' expertise, extensive training events for the authorities are also planned as part of a very extensive consultancy project with an external consultant in 2024/2025.

<u>Conclusion</u>: In summary, the vulnerability can be classified as medium (1.8).

<u>Money laundering</u>
In the summarised scenarios of the Supranational Risk Assessment, the vulnerability of insurance intermediaries with regard to misuse for money laundering purposes was classified as low/medium significant (1-2). The national vulnerability will be derived below.

(a) Risk potential:
The risk potential is considered to be relatively limited due to the overall strong regulation of the sector. In principle, however, life insurance products and investment products could lend themselves to terrorism financing, e.g. if foreign persons are beneficiaries of such insurance policies and funds could thus be transferred across borders.

(b) Risk awareness:

The fight against money laundering is the subject of training and further education for insurance intermediaries. Recently, various information events and awareness raising workshops have been held throughout Austria for tradespersons (as at October 2024, 8 by the BMAW with around 300 participants so far; others have been organised by other bodies, such as the FIU together with the Chamber), so it can be assumed that risk awareness has increased.

By continuing the far-reaching survey measures already mentioned and implemented in 2021, a further increase in risk awareness can be assumed and this is actually confirmed by the feedback from the trade authorities.

(c) legal framework and supervision/governance:
As part of the project with the external service provider, the legal framework and overall supervision in the commercial sector were comprehensively analysed. The points of criticism identified were used to formulate a corresponding action plan, the implementation of which will make it possible to improve the framework conditions and supervision.

Human and financial resources:
Equipping the authorities in terms of personnel resources and expertise was identified as a particularly important issue. With regard to the allocation of resources in this area, clear requests were made to those responsible in the federal states - where organisational responsibility lies - to increase the proportion of these funds for the AML/FT area from the total funds allocated to the federal states by the Federal Ministry of Finance in the financial equalisation scheme. In the past, this has already led to an increased use of funds by the federal states and should now be able to lead to a further improvement. Following feedback from the federal states, the number of FTEs was increased from 11 to 16 in 2024.

With regard to the authorities' expertise, extensive and detailed training events (around 16 workshops) are also planned for the authorities as part of the very extensive two-year consultancy project with an external consultant in 2024/2025.

<u>Conclusion</u>: In summary, the vulnerability can be classified as medium (1.9).

<u>Proliferation financing</u>

(a) Risk potential:
The risk of proliferation financing can generally be categorised as somewhat lower for capital-forming insurance products, as these tend to serve the long-term wealth accumulation of individuals.

(b) Risk awareness:
Various information events and awareness raising workshops have recently been held throughout Austria, including on proliferation financing (as of October 2024, 8 by the BMAW with around 300

participants so far; others have been organised by other agencies, such as the FIU together with the Chamber), so that it can be assumed that risk awareness has increased.

By continuing the far-reaching survey measures already mentioned and implemented in 2021, a further increase in risk awareness can be assumed and this is actually confirmed by the feedback from the trade authorities.

(c) legal framework and supervision/governance:
With Federal Law Gazette I No. 150/2024, an amendment to the Trade Act came into force on 6 January 2025, which also includes compliance with the obligations of tradespersons with regard to proliferation financing.

Human and financial resources:
Equipping the authorities in terms of personnel resources and expertise was identified as a particularly important issue. With regard to resources in this area, clear requests were made to those responsible in the federal states - who are responsible for the organisation - to increase the proportion of these funds for the AML/FT area from the total funds allocated to the federal states by the Federal Ministry of Finance in financial equalisation. In the past, this has already led to an increased use of funds by the federal states and should now be able to lead to a further improvement. Following feedback from the federal states, the number of FTEs was increased from 11 to 16 in 2024.

With regard to the authorities' expertise, extensive and detailed training events (around 16 workshops) are also planned for the authorities as part of the very extensive two-year consultancy project with an external consultant in 2024/2025.

Conclusion: In summary, the vulnerability is classified as low (1).

Risk minimisation measures

These have already been mentioned above. The two-year reorganisation and improvement project currently underway, which includes comprehensive measures, is of key importance.

Total risk

In summary, the overall risk is categorised as follows: **TF 1.7 (medium); ML 1.7 (medium); PF 1 (low).**

Recommendations

The measures already initiated with regard to the entire commercial administration in terms of centralisation and improved structuring and organisation and rationalisation of budget management and cooperation in this area and possibly beyond should be continued on an ongoing basis. The activities and measures planned by the EU as part of the sixth money laundering package should be integrated appropriately and mutual synergies should be sought.

15.2 Office services; Management consultants

General description
The sector is a regulated industry under Art. 94(74) Trade Act 1994 and its inclusion in the obligations to combat ML/TF is provided for in Art. 365m1(2)(3) Trade Act 1994. The enforcement reports of the trade authorities for 2023 assumed that around 34,000 companies potentially fell within the scope of the provisions. This is the number of tradespersons practising commercial professions that could potentially fall under the GWFTPF provisions (e.g. management consultants). However, due to the system of trade law with fixed professional definitions, the number of persons who actually carry out activities in accordance with the ML Directive is significantly lower. A risk survey is currently carried out every two years. The identification of risks from a criminological and typological perspective is currently mainly based on the findings and recommendations of the SNRA and the NRA as well as the law enforcement authorities and the FIU. The assessment of the respective company-related risks is carried out using a digital survey procedure.
Threat
Terrorism financing In the summarised scenarios of the Supranational Risk Assessment, the threat of management consultants/office service companies being misused for terrorist activities was classified as very significant (4). The national threat will be derived below. Threats exist in the case of management consultants in that they can be used to create international company structures that serve as a means of concealment. In the case of office service companies in particular, by providing foreign companies with registered offices that can be used to operate various front companies. These structures can be used in particular to transfer money. **Conclusion: In summary, the threat is classified as very high (4).**
Money laundering In the summarised scenarios of the Supranational Risk Assessment, the threat was classified as significant (3). The national threat will be derived below. There are threats from frequent remote transactions. Threats exist in the case of management consultants in that they can be used to create international company structures that serve as a means of concealment. In the case of office service companies in particular, by providing foreign companies with registered offices that can

be used to operate various front companies. These structures can be used in particular to transfer money.

Conclusion: In summary, the threat is classified as high (3).

Proliferation financing

There are threats from any advisory services that could be used to enable critical activities in the sense of proliferation financing, especially through the establishment of companies.

Conclusion: In summary, the threat is classified as low (1.5).

Vulnerability

Terrorism financing

In the summarised scenarios of the Supranational Risk Assessment, the vulnerability of business consultants/office service providers with regard to abuse for the purposes of terrorism financing was classified as significant (3). The national vulnerability will be derived below.

(a) Risk potential:

Threats exist with management consultants in that they can be used to create international company structures. In the case of office service companies in particular, by providing foreign companies with registered offices that can be used to operate various front companies. These constructs can be used in particular to transfer money. The vulnerability may result from the fact that the perpetrators operate so inconspicuously that the objective of terrorism financing is not easy to recognise.

(b) Risk awareness:

The fight against terrorism financing is the subject of training for business consultants. Various information events and awareness-raising workshops have recently been held throughout Austria (as at October 2024, 8 by the BMAW with around 300 participants so far; others have been organised by other bodies, such as the FIU together with the Chamber of Commerce), so that it can be assumed that risk awareness has increased.

By continuing the far-reaching survey measures already mentioned and implemented in 2021, a further increase in risk awareness can be assumed and this is actually confirmed by the feedback from the trade authorities.

(c) legal framework and supervision/governance:

As part of the project with the external service provider, the legal framework and overall supervision in the commercial sector were comprehensively analysed. The points of criticism identified were used to formulate a corresponding action plan, the implementation of which will make it possible to improve the framework conditions and supervision.

Human and financial resources:
Equipping the authorities in terms of personnel resources and expertise was identified as a particularly important issue. With regard to resources in this area, clear requests were made to those responsible in the federal states where organisational responsibility lies to increase the allocation of existing funds to this area of AML/CFT/PF. With regard to the authorities' expertise, extensive training events for the authorities are also planned as part of a very extensive consultancy project with the external consultant in 2024/2025. Following feedback from the federal states, the number of FTEs was increased from 11 to 16 in 2024.

Conclusion: In summary, the vulnerability is classified as medium (2.3).

Money laundering
In the summarised scenarios of the Supranational Risk Assessment, the vulnerability of business consultants/office service providers with regard to misuse for money laundering purposes was classified as significant (3). The national vulnerability will be derived below.

(a) Risk potential:
Threats exist with management consultants in that they can be used to create international company structures. In the case of office service companies in particular, by providing foreign companies with registered offices that can be used to operate various front companies. These constructs can be used in particular to transfer money. The vulnerability may result from the fact that the perpetrators operate so inconspicuously that the objective of the money laundering is not easy to recognise.

(b) Risk awareness:
The fight against money laundering is the subject of training for business consultants. Various information events and awareness-raising workshops have recently been held throughout Austria (as at October 2024, 8 by the BMAW with around 300 participants to date; others have been organised by other bodies, such as the FIU together with the Chamber of Commerce), so that it can be assumed that risk awareness has increased.

By continuing the far-reaching survey measures already mentioned and implemented in 2021, a further increase in risk awareness can be assumed and this is actually confirmed by the feedback from the trade authorities.

(c) legal framework and supervision/governance:
As part of the project with the external service provider, the legal framework and overall supervision in the commercial sector were comprehensively analysed. The points of criticism identified were used to formulate a corresponding action plan, the implementation of which will make it possible to improve the framework conditions and supervision.

Human and financial resources:

Equipping the authorities in terms of personnel resources and expertise was identified as a particularly important issue. With regard to resources in this area, clear requests were made to those responsible in the federal states where organisational responsibility lies to increase the allocation of existing funds to this area of AML/CFT/PF. With regard to the authorities' expertise, extensive training events for the authorities are also planned as part of a very extensive consultancy project with the external consultant in 2024/2025. Following feedback from the federal states, the number of FTEs was increased from 11 to 16 in 2024.

Conclusion: In summary, the vulnerability can be classified as medium (2.4).

Proliferation financing

(a) Risk potential:
Threats exist with management consultants in that they can be used to create international company structures. In the case of office service companies in particular, by providing foreign companies with registered offices that can be used to operate various front companies. These constructs can be used in particular to transfer money. The vulnerability may result from the fact that the perpetrators operate so inconspicuously that the objective of the money laundering is not easy to recognise.

(b) Risk awareness:
Various information events and awareness-raising workshops have recently been held throughout Austria (as at October 2024, the BMAW has organised 8 so far with around 300 participants; others have been organised by other bodies, such as the FIU together with the Chamber), so it can be assumed that risk awareness has increased.

By continuing the far-reaching survey measures already mentioned and implemented in 2021, a further increase in risk awareness can be assumed and this is actually confirmed by the feedback from the trade authorities.

(c) legal framework and supervision/governance:
As part of the project with the external service provider, the legal framework and overall supervision in the commercial sector were comprehensively analysed. The points of criticism identified were used to formulate a corresponding action plan, the implementation of which will make it possible to improve the framework conditions and supervision.

Human and financial resources:

Equipping the authorities in terms of human resources and expertise was identified as a particularly important issue. With regard to resources in this area, clear calls were made to those

responsible in the countries where organisational responsibility lies to extend the allocation from existing funds to the field of proliferation financing. With regard to the authorities' expertise, extensive training events for the authorities are also planned as part of a very extensive consultancy project with the external consultant in 2024/2025. Following feedback from the federal states, the number of FTEs was increased from 11 to 16 in 2024.

Conclusion: In summary, the vulnerability can be classified as low (1.5).

Risk minimisation measures
See above; key measure the two-year advisory and restructuring project 2023 - 2025.
Total risk TF
In summary, the overall risk is categorised as follows: **TF: medium 2.7; ML: medium 2.4; PF: low 1.4.**
Recommendations
The measures already initiated with regard to the entire commercial administration in terms of centralisation and improved structuring and organisation and rationalisation of budget management and cooperation in this area and possibly beyond should be continued on an ongoing basis. The activities and measures planned by the EU as part of the sixth money laundering package should be integrated appropriately and mutual synergies should be sought.

15.3 Trade incl. auctioneers

a) Antiques and works of art

General description
The sector is subject to the Trade Act (GewO) 1994, although in principle there are no specific qualification requirements (free trade). Its inclusion in the obligations to combat ML/TF is provided for in Art. 365m1 para. 2 no. 1 GewO 1994. The provisions cover trafficking as a whole. In order to enable risk-based enforcement in line with the FATF provisions, a focus is placed on antiques, art, motor vehicles, precious metals, precious stones, crude oil and weapons. In addition, with the exception of the art trade (including non-cash transactions), only traders who carry out cash transactions of EUR 10,000 or more are covered.

The enforcement reports of the trade authorities for 2024 assumed a total of around 24,000 companies in trade that potentially fell within the scope of the provisions. Of these, at most around half actually fall within the scope of application.

A risk survey is carried out every two years using a digital questionnaire to identify individual company risks and derive regional and sectoral risks. The identification of risks from a criminological and typological perspective is currently mainly based on the findings and recommendations of the SNRA and the NRA as well as the law enforcement authorities and the FIU.

Threat

Terrorism financing

In the summarised scenarios of the Supranational Risk Assessment, the threat of traders being misused for terrorist activities was classified as moderately significant (2). The national threat will be derived below.

The relatively large number of long-distance transactions and the relatively high proportion of cash transactions pose a threat. A concrete threat is posed by terrorist organisations selling art goods from their countries internationally in order to finance themselves.

Conclusion: In summary, the threat is classified as medium (2)

Money laundering

In the summarised scenarios of the Supranational Risk Assessment, the threat was classified as moderately significant (2). The national threat will be derived below.

Threats exist due to the relatively large number of long-distance transactions and the relatively high proportion of cash transactions as well as the high-priced and valuable goods sold by traders to walk-in customers. This in turn offers the opportunity to invest a large sum of cash in items of secure value and thus launder money. A typical scenario is the investment of illicit assets in valuable goods that are easy to move, retain their value and are easy to utilise in order to increase the distance between the illicit source and the utilisation or use of the assets and to use this for concealment.

Conclusion: In summary, the threat is classified as high (3).

Proliferation financing

As with terrorism financing, the most likely threat in the antiquities trade could be that antiquities or art from one of the problem states could be to finance dangerous military programmes.

Conclusion: In summary, the threat is classified as low (1.5).

Vulnerability

Terrorism financing

In the summarised scenarios of the Supranational Risk Assessment, the vulnerability of traders in antiques and works of art with regard to misuse for the purposes of terrorism financing was classified as very significant (4). The national vulnerability will be derived below.

(a) Risk potential:

Traders in antiques and works of art pose a threat in that they can be used to sell certain works of art from certain high-risk countries and thus generate funds for terrorist acts.

(b) Risk awareness:

Various information events and awareness-raising workshops have recently been held throughout Austria (as at October 2024, the BMAW has organised 8 to date with around 300 participants; others have been organised by other bodies, such as the FIU together with the Chamber of Commerce), so that it can be assumed that risk awareness has increased. The annual money laundering days can also be mentioned here.

By continuing the far-reaching survey measures already mentioned and implemented in 2021, a further increase in risk awareness can be assumed and this is actually confirmed by the feedback from the trade authorities.

(c) legal framework and supervision/governance:

As part of the project with the external service provider, the legal framework and overall supervision in the commercial sector were comprehensively analysed. The points of criticism identified were used to formulate a corresponding action plan, the implementation of which will make it possible to improve the framework conditions and supervision.

Human and financial resources:

Equipping the authorities in terms of human resources and expertise was identified as a particularly important issue. With regard to the allocation of resources in this area, clear requests were made to those responsible in the federal states where organisational responsibility lies to increase the allocation of existing funds to this area of AML/FT. With regard to the authorities' expertise, extensive training events for the authorities are also planned as part of a very extensive consultancy project with the external consultant in 2024/2025.
Following feedback from the federal states, the number of FTEs was increased from 11 to 16 in 2024.

Conclusion: In summary, the vulnerability with regard to terrorism financing in the trade in antiques and works of art is classified as high (2.8).

Money laundering

In the summarised scenarios of the Supranational Risk Assessment, the vulnerability of traders in antiques and works of art with regard to misuse for the purposes of money laundering was classified as very significant (4). The national vulnerability will be derived below.

(a) Risk potential:

Traders in antiques and works of art pose a threat in that they can be used to sell certain works of art from certain high-risk countries and thus generate funds for terrorist acts.

(b) Risk awareness:

Various information events and awareness-raising workshops have recently been held throughout Austria (as at October 2024, the BMAW has organised 8 to date with around 300 participants; others have been organised by other bodies, such as the FIU together with the Chamber of Commerce), so that it can be assumed that risk awareness has increased. The annual money laundering days can also be mentioned here.

By continuing the far-reaching survey measures already mentioned and implemented in 2021, a further increase in risk awareness can be assumed and this is actually confirmed by the feedback from the trade authorities.

(c) legal framework and supervision/governance:

As part of the project with the external service provider, the legal framework and overall supervision in the commercial sector were comprehensively analysed. The points of criticism identified were used to formulate a corresponding action plan, the implementation of which will make it possible to improve the framework conditions and supervision.

Human and financial resources:

Equipping the authorities in terms of human resources and expertise was identified as a particularly important issue. With regard to the allocation of resources in this area, clear requests were made to those responsible in the federal states where organisational responsibility lies to increase the allocation of existing funds to this area of AML/FT. With regard to the authorities' expertise, extensive training events for the authorities are also planned as part of a very extensive consultancy project with the external consultant in 2024/2025.
Following feedback from the federal states, the number of FTEs was increased from 11 to 16 in 2024.

Conclusion: To summarise, the vulnerability of traders in antiques and works of art with regard to money laundering is high **(2.9).**

Proliferation financing

(a) Risk potential:
The risk potential essentially results from the conceivable scenarios. The danger of weapons of mass destruction, delivery systems, dual-use goods and the corresponding know-how coming into the possession of sanctioned regimes or terrorist organisations, or of certain goods being misused for proliferation-relevant purposes contrary to official statements, represents one of the main proliferation-related threats. In this context, Austria is not only a transit country for proliferation-relevant goods, but also a target country for illegal procurement activities due to its highly developed industrial production and the large number of small and medium-sized enterprises, which are world leaders in some areas. Dual-use goods, i.e. materials or products that can be used in both civil and military applications due to their high level of development, pose a particular problem.

However, antiques and works of art are not primarily suitable for armouring purposes.

(b) Risk awareness:
Here, too, reference should be made to the ongoing awareness events. This should make it possible to reduce risks here and in the future.

(c) legal framework and supervision/governance:
As above; new legal provisions

Human and financial resources:
Major problem, currently being addressed.
Following feedback from the federal states, the number of FTEs was increased from 11 to 16 in 2024.

Conclusion: In summary, the vulnerability is classified as low (1.5).

Risk minimisation measures
Ongoing project
Total risk
In summary, the overall risk is categorised as follows: **TF: medium (2.2); ML: medium (2.3); PF: low (1.4).**
Recommendations
Ongoing project see above

b) Precious metals and precious stones

General description
The sector is subject to the Trade Act (GewO) 1994, although in principle there are no specific qualification requirements (free trade). Its inclusion in the obligations to combat AML/CFT/PF is provided for in Art. 365m1 para. 2 no. 1 GewO 1994. The provisions cover trade as a whole. In order to enable risk-based enforcement in accordance with the FATF provisions, a focus is placed on antiques, art, motor vehicles, precious metals, precious stones, crude oil and weapons. In addition, with the exception of the art trade (which also includes non-cash transactions), only traders who carry out cash transactions of EUR 10,000 or more are covered. The enforcement reports of the trade authorities for 2024 assumed a total of around 24,000 companies in trade that potentially fell within the scope of the provisions. Around half of these actually fall under the provisions at most. A risk survey is carried out every two years. The identification of risks from a criminological and typological perspective is currently mainly based on the findings and recommendations of the SNRA and the NRA as well as the law enforcement authorities and the FIU.
Threat
Terrorism financing In the summarised scenarios of the Supranational Risk Assessment, the threat of traders in precious metals and gemstones being misused for terrorist activities was classified as moderately significant (3). The national threat will be derived below. The relatively large number of long-distance transactions and the relatively high proportion of cash transactions pose a threat. Precious metals and gemstones are generally suitable as a means of financing terrorist activities due to their small size and high intrinsic value. **Conclusion: In summary, the threat is classified as high (3)**
Money laundering In the summarised scenarios of the Supranational Risk Assessment, the threat was classified as very significant (4). The national threat will be derived below. Threats exist due to the relatively large number of long-distance transactions and the relatively high proportion of cash transactions as well as the high-priced and valuable goods sold by traders to walk-in customers. This in turn offers the opportunity to invest a large sum of cash in items of secure value and thus launder money. Precious metals and gemstones are generally suitable for money laundering due to their small size and high intrinsic value and can be classified as high risk.

Several scenarios have been reported from Vienna and other federal states in which advertisements are frequently published offering gold, jewellery and fur purchases. These businesses are problematic in that they work almost exclusively with cash. These businesses are rented in hotels for a few days, the operators are often not identifiable and some do not have a business licence or have one abroad. Since 2023, 34 checks have been carried out in this regard, resulting in a total of 43 reports. The consistent inspections carried out by the Market Office have led to this type of business activity disappearing from Vienna's urban area. There have also been reports of problematic purchases by traders. These problems are continuously monitored in connection with the individual cases, particularly with regard to possible people behind them.

Conclusion: In summary, the threat is classified as very high (4).

Proliferation financing

Threats exist in a similar way to the antiques and art trade, but with the exception of the possibility of retrofitting historical weapons.

Conclusion: In summary, the threat is classified as medium (2.5).

Vulnerability

Terrorism financing

In the summarised scenarios of the Supranational Risk Assessment, the vulnerability of traders in precious metals and gemstones was classified as very significant (4) with regard to misuse for the purposes of terrorism financing. The national vulnerability will be derived below.

(a) Risk potential:

Traders in antiques and works of art pose a threat in that they can be used to sell certain works of art from certain high-risk countries and thus generate funds for terrorist acts.

(b) Risk awareness:

Various information events and awareness-raising workshops have recently been held throughout Austria (as at October 2024, 8 by the BMAW with around 300 participants so far; others have been organised by other bodies, such as the FIU together with the Chamber of Commerce), so it can be assumed that risk awareness has increased. The annual money laundering days can also be mentioned here.

By continuing the far-reaching survey measures already mentioned and implemented in 2021, a further increase in risk awareness can be assumed and this is actually confirmed by the feedback from the trade authorities.

(c) legal framework and supervision/governance:

As part of the project with the external service provider, the legal framework and overall supervision in the commercial sector were comprehensively analysed. The points of criticism identified were used to formulate a corresponding action plan, the implementation of which will make it possible to improve the framework conditions and supervision.

Human and financial resources:
Equipping the authorities in terms of human resources and expertise was identified as a particularly important issue. With regard to the allocation of resources in this area, clear requests were made to those responsible in the countries where organisational responsibility lies to increase the allocation from existing funds to this area of AML/FT/PF. With regard to the authorities' expertise, extensive training events for the authorities are also planned as part of a very extensive consultancy project with the external consultant in 2024/2025.
Following feedback from the federal states, the number of FTEs was increased from 11 to 16 in 2024.

Conclusion: In summary, vulnerability is rated as high (2.8).

Money laundering
In the summarised scenarios of the Supranational Risk Assessment, the vulnerability of traders in precious metals and gemstones with regard to misuse for the purposes of money laundering was classified as significant (3). The national vulnerability will be derived below.

(a) Risk potential:
Traders of precious metals and gemstones pose a threat in that they can be used to sell precious metals and gemstones from certain high-risk countries and thus generate funds for terrorist acts.

(b) Risk awareness:
Various information events and awareness-raising workshops have recently been held throughout Austria (as at October 2024, 8 by the BMAW with around 300 participants so far; others have been organised by other bodies, such as the FIU together with the Chamber of Commerce), so it can be assumed that risk awareness has increased. The annual money laundering days can also be mentioned here.

By continuing the far-reaching survey measures already mentioned and implemented in 2021, a further increase in risk awareness can be assumed and this is actually confirmed by the feedback from the trade authorities.

(c) legal framework and supervision/governance:
As part of the project with the external service provider, the legal framework and overall supervision in the commercial sector were comprehensively analysed. The points of criticism identified were used to formulate a corresponding action plan, the implementation of which will make it possible to improve the framework conditions and supervision.

Human and financial resources:
Equipping the authorities in terms of human resources and expertise was identified as a particularly important issue. With regard to resources in this area, clear requests were made to those responsible in the federal states where organisational responsibility lies to increase the allocation from existing funds to this area of AML/FT. The feedback from the federal states indicates an increase from approx. 11 to 16 FTEs for 2024. With regard to the authorities' expertise, extensive training events for the authorities are also planned as part of a very extensive consultancy project with the external consultant in 2024/2025.

Conclusion: To summarise, the vulnerability of traders in precious metals and gemstones **can be classified as high (3).**

Proliferation financing

(a) Risk potential:
The risk potential essentially results from the conceivable scenarios. Precious metals and gemstones are not primarily suitable for defence purposes, unless they have special technical applications (e.g. industrial diamonds for drilling tools).

(b) Risk awareness:
Here, too, reference should be made to the ongoing awareness events. This should make it possible to reduce risks here and in the future.

(c) legal framework and supervision/governance:
As above; new legal provisions

Human and financial resources:
Major problem, currently being addressed.

Conclusion: In summary, the vulnerability is classified as medium (2).

Risk minimisation measures

As above

Total risk

In summary, the overall risk is categorised as follows: **TF high (2.6); ML high (2.8); PF medium (2.0).**

Recommendations

As above

c) High-priced goods - other than precious metals and precious stones

General description

The sector is subject to the Trade Act (GewO) 1994, although in principle there are no specific qualification requirements (free trade).

Its inclusion in the obligations to combat ML/TF is provided for in Art. 365m1 para. 2 no. 1 GewO 1994. The provisions cover trafficking as a whole. In order to enable risk-based enforcement in accordance with the FATF provisions, a focus is placed on antiques, art, motor vehicles, precious metals, precious stones, crude oil and weapons. In addition, with the exception of the art trade, only traders who carry out transactions of EUR 10,000 or more are covered.

The enforcement reports of the trade authorities for 2024 assumed a total of around 24,000 companies in trade that potentially fell within the scope of the provisions. In reality, the provisions apply to no more than half of these.

A digital risk survey is carried out every two years at company level and aggregated at district, state and federal level and by sector. The identification of risks from a criminological and typological perspective is currently mainly based on the findings and recommendations of the SNRA and the NRA as well as the law enforcement authorities and the FIU.

Threat

Terrorism financing

In the summarised scenarios of the Supranational Risk Assessment, the threat of other traders of valuable goods being misused for terrorist activities was not classified as relevant.

As a result, the national threat is to be reconsidered.

The relatively large number of long-distance transactions and the relatively high proportion of cash transactions pose a fundamental threat.

Conclusion: In summary, the threat can be classified as low (1)

Money laundering

In the summarised scenarios of the Supranational Risk Assessment, the threat of other traders of valuable goods being used for money laundering was classified as significant (3). The national threat will be derived below.

The relatively large number of long-distance transactions and the relatively high proportion of cash transactions pose a threat. Valuable goods are generally suitable for quickly tying up large sums of money. They can therefore be used to transfer assets to conceal the illegal origin of assets, especially if they are easy to move.

Conclusion: In summary, the threat is classified as high (3).

Proliferation financing

The risks here are similar to those for other traders. Clearly, components of defence equipment are particularly suitable. Conceivable would be electrotechnical goods or chemical products, weapons and weapon components, operating materials.

Conclusion: In summary, the threat is classified as high (3).

Vulnerability

Terrorism financing

In the summarised scenarios of the Supranational Risk Assessment, the vulnerability of traders of other valuable goods to being misused for terrorism financing purposes was not identified as relevant.

The national vulnerability is to be indicated below.

(a) Risk potential:

There is less of a threat to traders of other valuable goods, as large sums of money do not necessarily have to be invested with regard to terrorism financing, but rather the mobility of goods for the purpose of local realisability is more relevant.

(b) Risk awareness:

Various information events and awareness-raising workshops have recently been held throughout Austria (as at October 2024, 8 by the BMAW with around 300 participants so far; others have been organised by other bodies, such as the FIU together with the Chamber of Commerce), so it can be assumed that risk awareness has increased. The annual money laundering days can also be mentioned here.

By continuing the far-reaching survey measures already mentioned and implemented in 2021, a further increase in risk awareness can be assumed and this is actually confirmed by the feedback from the trade authorities.

(c) legal framework and supervision/governance:

As part of the project with the external service provider, the legal framework and overall supervision in the commercial sector were comprehensively analysed. The points of criticism identified were used to formulate a corresponding action plan, the implementation of which will make it possible to improve the framework conditions and supervision.

Human and financial resources:

Equipping the authorities in terms of human resources and expertise was identified as a particularly important issue. With regard to resources in this area, clear requests were made to those responsible in the federal states where organisational responsibility lies to increase the

allocation of existing funds to this area of AML/FT. As already mentioned elsewhere, feedback from the federal states also led to an increase from 11 FTEs to 16 in 2024. With regard to the authorities' expertise, extensive training events for the authorities are also planned as part of a very extensive consultancy project with the external consultant in 2024/2025.

Conclusion: In summary, the vulnerability can be classified as medium (1.7).

Money laundering

In the summarised scenarios of the Supranational Risk Assessment, the vulnerability of traders of other valuable goods with regard to misuse for the purposes of money laundering was classified as significant (3). The national vulnerability will be derived below.

(a) Risk potential:

Traders of other valuable goods pose a threat in that all such goods are suitable for the investment of funds from illegal sources.

(b) Risk awareness:

Various information events and awareness-raising workshops have recently been held throughout Austria (as of October 2024, the BMAW has organised 8 to date with around 300 participants; others have been organised by other bodies, such as the FIU together with the Chamber of Commerce), so that it can be assumed that risk awareness has increased. The annual money laundering days can also be mentioned here.

By continuing the far-reaching survey measures already mentioned and implemented in 2021, a further increase in risk awareness can be assumed and this is actually confirmed by the feedback from the trade authorities.

(c) legal framework and supervision/governance:

As part of the project with the external service provider, a comprehensive analysis of the legal framework and overall supervision in the commercial sector was carried out. The points of criticism identified were used to formulate a corresponding action plan, the implementation of which will make it possible to improve the framework conditions and supervision.

Human and financial resources:

Equipping the authorities in terms of human resources and expertise was identified as a particularly important issue. With regard to the allocation of resources in this area, clear requests were made to those responsible in the federal states where organisational responsibility lies to increase the allocation from the available funds to this area of AML/FT (see elsewhere: 16 FTEs were now reported in 2024 instead of the previous approx. 11). With regard to the authorities' expertise, extensive training events for the authorities are also planned as part of a very extensive consultancy project with the external consultant in 2024/2025.

Conclusion: In summary, the vulnerability of traders of other valuable goods **can be classified as medium (2.5).**

Proliferation financing

(a) Risk potential:
Threats exist for traders of other valuable goods in that some of them are suitable for armaments activities.

(b) Risk awareness:
Various information events and awareness-raising workshops have recently been held for the commercial sector throughout Austria (as of October 2024, 8 to date by the BMAW with around 300 participants; others have been organised by other bodies, such as the FIU together with the Chamber of Commerce), so that it can be assumed that risk awareness has increased. The annual money laundering days can also be mentioned here.

By continuing the far-reaching survey measures already mentioned and implemented in 2021, a further increase in risk awareness can be assumed and this is actually confirmed by the feedback from the trade authorities.

(c) legal framework and supervision/governance:
As part of the project with the external service provider, a comprehensive analysis of the legal framework and overall supervision in the commercial sector was carried out. The points of criticism identified were used to formulate a corresponding action plan, the implementation of which will make it possible to improve the framework conditions and supervision.

Human and financial resources:

Equipping the authorities in terms of human resources and expertise was identified as a particularly important issue. With regard to resources in this area, clear requests were made to those responsible in the federal states where organisational responsibility lies to increase the allocation from existing funds to this area of AML/FT (see above: increase in 2024 from approx. 11 to 16 FTEs). With regard to the authorities' expertise, extensive training events for the authorities are also planned as part of a very extensive consultancy project with the external consultant in 2024/2025.

Conclusion: In summary, the vulnerability of traders of other valuable goods **can be classified as medium (2.5)**

Risk minimisation measures

Ongoing project, see above.
Total risk
In summary, the overall risk can be categorised as follows: **TF low (1.3); ML medium (2.4); PF medium (2.4).**
Recommendations
The recommendations are aimed at the authorities and include suggestions on how to improve the prevention of ML/TF.

15.4 Real estate agents

General description
The sector is a regulated industry pursuant to Art. 94 Z 35 Trade Act (GewO) 1994. Its inclusion in the obligations to combat ML/TF is provided for in Art. 365m1 para. 2 Z2 GewO 1994. The enforcement reports of the trade authorities for 2023 assumed that around 6,000 companies would fall within the scope of the provisions. **Cases:** Problematic cases have recently been publicised in the sector. As far as can be seen from the public perception so far, these cases involved extensive corporate networks and various problematic activities. Various people were apparently harmed. Comprehensive criminological and procedural investigations are being carried out. Every two years, a risk survey is carried out at company level, which is aggregated to the geographical and sectoral units. The identification of threats from a criminological and typological perspective is currently mainly based on the findings and recommendations of the SNRA and the NRA as well as law enforcement agencies and the FIU.
Threat
Terrorism financing In the summarised scenarios of the Supranational Risk Assessment, the threat of estate agents being misused for terrorist activities was classified as very significant (4). The national threat will be derived below. Possible scenarios include the procurement of land and property directly as bases for terrorist activities.

Conclusion: In summary, the threat is classified as very high (4).

Money laundering

In the summarised scenarios of the Supranational Risk Assessment, the threat was classified as very significant (4). The national threat will be derived below.

There are threats from various potential criminal processes. In particular, property is suitable as the first stage of money laundering due to its potentially high value.

Here, too, mention can be made of all the events surrounding the cases mentioned above, which are currently being comprehensively investigated by the courts and authorities.

Conclusion: In summary, the threat is classified as very high (4).

Proliferation financing

Threats here typically arise from the possible use of real estate investments for defence activities.

Conclusion: In summary, the threat is classified as medium (2.5).

Vulnerability

Terrorism financing

In the summarised scenarios of the Supranational Risk Assessment, the vulnerability of estate agents with regard to abuse for the purposes of terrorism financing was classified as very significant (4). The national vulnerability will be derived below.

(a) Risk potential:

Estate agents pose a threat insofar as all such assets are suitable for the investment of funds for later use for terrorist purposes, or may also serve directly as a starting point for terrorist activities.

(b) Risk awareness:

Various information events and awareness-raising workshops have recently been held for commercial companies throughout Austria (as at October 2024, 8 by the BMAW with around 300 participants so far; others have been organised by other bodies, such as the FIU together with the Chamber of Commerce), so it can be assumed that risk awareness has increased. The annual money laundering days can also be mentioned here.

By continuing the far-reaching survey measures already mentioned and implemented in 2021, a further increase in risk awareness can be assumed and this is actually confirmed by the feedback from the trade authorities.

(c) legal framework and supervision/governance:
As part of the project with the external service provider, the legal framework and overall supervision in the commercial sector were comprehensively analysed. The points of criticism identified were used to formulate a corresponding action plan, the implementation of which will make it possible to improve the framework conditions and supervision.

Human and financial resources:

Equipping the authorities in terms of human resources and expertise was identified as a particularly important issue. With regard to resources in this area, clear requests were made to those responsible in the federal states where organisational responsibility lies to increase the allocation from existing funds to this area of AML/FT (see above; increase from 11 to 16 FTEs in 2024). With regard to the authorities' expertise, extensive training events for the authorities are also planned as part of a very extensive consultancy project with the external consultant in 2024/2025.

Conclusion: In summary, vulnerability is rated as high (2.7).

Money laundering
In the summarised scenarios of the Supranational Risk Assessment, the vulnerability of estate agents with regard to abuse for the purposes of money laundering was classified as very significant (4). The national vulnerability will be derived below.

(a) Risk potential:
Threats exist for estate agents insofar as all properties are suitable for the investment of larger funds from illegal activities, essentially because of their high prices.

(b) Risk awareness:
Various information events and awareness-raising workshops have recently been held throughout Austria (as at October 2024, the BMAW has organised 8 to date with around 300 participants; others have been organised by other bodies, such as the FIU together with the Chamber of Commerce), so that it can be assumed that risk awareness has increased. The annual money laundering days can also be mentioned here.

By continuing the far-reaching survey measures already mentioned and implemented in 2021, a further increase in risk awareness can be assumed and this is actually confirmed by the feedback from the trade authorities.

(c) legal framework and supervision/governance:
As part of the project with the external service provider, the legal framework and overall supervision in the commercial sector were comprehensively analysed. The points of criticism

identified were used to formulate a corresponding action plan, the implementation of which will make it possible to improve the framework conditions and supervision.

Human and financial resources:

Equipping the authorities in terms of human resources and expertise was identified as a particularly important issue. With regard to resources in this area, clear requests were made to those responsible in the federal states where organisational responsibility lies to increase the allocation of existing funds to this area of AML/FT (see above). With regard to the authorities' expertise, extensive training events for the authorities are also planned as part of a very extensive consultancy project with the external consultant in 2024/2025.

Conclusion: In summary, the vulnerability can be classified as high (2.8).

Proliferation financing

(a) Risk potential:
Cf. previously

(b) Risk awareness:
Cf. previously

(c) legal framework and supervision/governance:
Cf. previously

Human and financial resources:
Cf. previously

Conclusion: In summary, the vulnerability is classified as medium (2.5).

Risk minimisation measures

Cf. previously

Total risk

In summary, the overall risk is categorised as follows: **TF high (2.9); ML high (3); PF medium (2.3).**

Recommendations

The recommendations are aimed at the authorities and include suggestions on how to improve the prevention of ML/TF.

	SNRA	Dashboard (vulnerability only)	NRA - Risk before risk minimisation measures	Total risk
Insurance intermediaries				
Threat				
TF	2,0	2,0	2,0	
ML	2,0	2,0	2,0	
PF	1,0	1,0	1,0	
Vulnerability				
TF	1,5	2,0	1,8	
ML	1,5	2,1	1,9	
PF	1,0	1,0	1,0	
total				
TF	1,7		**1,9**	1,7
ML	1,7		**1,9**	1,7
PF	1,0		1,0	1,0
Management consultant				
Threat				
TF	4,0	4,0	4,0	
ML	3,0	3,0	3,0	
PF	1,5	1,5	1,5	
Vulnerability				
TF	3,0	2,0	2,3	
ML	3,0	2,0	2,4	
PF	1,5	1,5	1,5	
total				

TF			3,0	2,7
ML			2,6	2,4
PF			1,5	1,4
Trade				
Antiques and art				
Threat				
TF	2,0	2,0	2,0	
ML	2,0	2,0	2,0	
PF	1,5	1,5	1,5	
Vulnerability				
TF	4,0	2,1	2,8	
ML	4,0	2,3	2,9	
PF	1,5	1,5	1,5	
total				
TF			**2,5**	2,2
ML			2,5	2,3
PF			1,5	1,4
Gold and precious metal				
Threat				
TF	3,0	3,0	3,0	
ML	4,0	4,0	4,0	
PF	2,5	2,5	2,5	
Vulnerability				
TF	4,0	2,1	2,8	
ML	3,0	2,3	2,5	
PF	2,0	2,0	2,0	
total				
TF			2,9	2,6
ML			3,1	2,8

PF			2,2	2,0
Other valuable goods				
Threat				
TF	1,0	1,0	1,0	
ML	3,0	3,0	3,0	
PF	3,0	3,0	3,0	
Vulnerability				
TF	1,0	2,1	1,7	
ML	3,0	2,3	2,5	
PF	2,5	2,5	2,5	
total				
TF			**1,4**	1,3
ML			**2,7**	2,4
PF			2,7	2,4
Real estate agents				
Threat				
TF	4,0	4,0	4,0	
ML	4,0	4,0	4,0	
PF	2,5	2,5	2,5	
Vulnerability				
TF	4,0	2,0	2,7	
ML	4,0	2,1	2,8	
PF	2,5	2,5	2,5	
total				
TF			**3,2**	2,9
ML			**3,3**	3,0
PF			2,5	2,3
PF - Figures based on assumptions and input DSN				

16 Sectoral risk assessment of non-profit organisations

General description
General information on sector / product / service / activity: This risk assessment is an abridged and updated version of the NPOs 2024 sectoral risk assessment. It is based on the current recommendation of the United Nations (UN Department of Economic and Social Affairs, 2018) on the internationally standardised definition of non-profit organisations (NPOs). NPOs are therefore defined as all • organisations registered as legal entities, • which are legally prevented from distributing any profits generated to members, managers or investors, • are legally autonomous, • are voluntary and • belong to the private sector, i.e. are not state-controlled, understood. In Austria (and many other countries), NPOs do not have their own legal form; they can be associations, foundations, limited liability companies, co-operatives and even (in fact, in exceptional cases) public limited companies. NPOs are often non-profit organisations. In Austria, however, the concept of non-profit status is primarily anchored in tax law. In special cases, such as federal or provincial foundations and funds, the legislator standardises non-profit status. There are around 135,000 NPOs in Austria that cover a wide range of services. Associations are the main legal form for non-profit organisations, as they can be established easily and with minimal capital investment. In 2025, 134,648 associations were registered in Austria, i.e. over 95% of NPOs are associations. The donation purposes cover a broad spectrum. Around 63% of donations (just under € 650 million) can be attributed to social projects in the broadest sense of the FATF definition.[13]

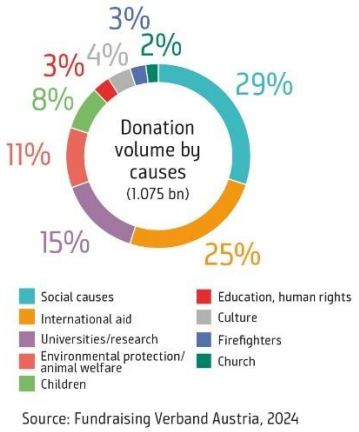
[13] Fundraising Association Austria. (2024), p. 5. *2024 Donation Report*. Retrieved 20 March 2025, from https://www.fundraising.at/wp-content/uploads/2024/12/FVA-Spendenbericht-2024.pdf. A service NPO as defined in the FATF Glossary is a "legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types "good works".

The social breadth of charitable activity in Austria contrasts with a strong concentration of financial flows. In international comparison, the volume of donations is much more focused on a small number of well-known organisations that have been audited by independent external bodies (Chamber of Tax Consultants and Auditors, Austrian Development Agency, European Commission). This is due to the recognisability of the major brands, the relatively small market, tax deductibility and the specific fundraising opportunities that are sometimes available to large NPOs (e.g. the ORF projects "Österreich hilft Österreich", "Nachbar in Not" and "Licht ins Dunkel").

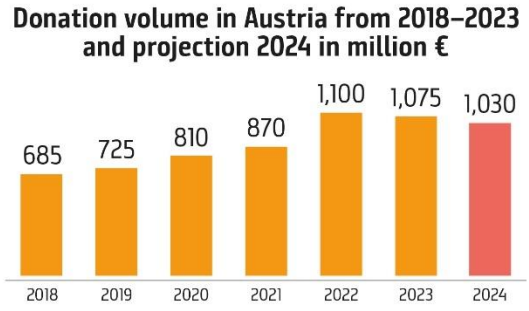
This trend has become even more pronounced in recent years. In 2023, the 100 largest NPOs received 75.4% of all donations made to civil society organisations. The largest Austrian NPO has a donation volume more than ten times higher than the NPO in 16th place and a donation volume more than a hundred times higher than the NPO in 100th place.[14] The high concentration of donations among a relatively small group of large, professionally structured and multi-audited NPOs is an important contextual factor for the assessment of sector risk.

A survey by the Fundraising Association Austria shows that donations totalled € 1,075 million in 2023, with 75% of the donations collected being used for activities in Austria and 25% for international aid. [15]

In total, 94% of all donations to NPOs in Austria are audited as part of an audit of the raising and use of funds, and 75% of all donations are subject to an in-depth audit by the Austrian Donation Seal of Quality.[16]



Source: Fundraising Verband Austria, 2024



Source: Fundraising Verband Austria, 2024

[14] Fundraising Association Austria. (2024), p. 30-31. *2024 Donation Report*. Retrieved 20 March 2025, from https://www.fundraising.at/wp-content/uploads/2024/12/FVA-Spendenbericht-2024.pdf
[15] Fundraising Association Austria. (2024), p. 5. *2024 Donation Report*. Retrieved 20 March 2025, from https://www.fundraising.at/wp-content/uploads/2024/12/FVA-Spendenbericht-2024.pdf
[16] Fundraising Association Austria. (2024), p. 32. *2024 Donation Report*. Retrieved 20 March 2025, from https://www.fundraising.at/wp-content/uploads/2024/12/FVA-Spendenbericht-2024.pdf

The sectoral risk assessment follows the FATF's differentiated approach and distinguishes between organisational and sectoral risks. Organisational risks affect, at least in the abstract, the overwhelming majority of NPOs that their activities lawfully. Organisational vulnerabilities can lead to abuse and thus to the terrorism financing of such NPOs, especially in risk situations such as operating in unstable third countries. Sectoral risks are posed by NPOs that deliberately engage in terrorism financing.

Threat

Organisational risks

In the summarised scenarios of the Supranational Risk Assessment, the threat of abuse for terrorism financing for NPOs that collect or transfer funds was classified as medium. For NPOs that receive institutional funding, including from the EU or from Member States responsible for managing EU funds, the threat was assessed as **low**.

The threat situation with regard to organisational risks was assessed by means of two risk surveys in the NPO sector in 2023 and 2024. The survey followed a functional approach and defined two risk groups:

- Countries on the FATF lists or the European Commission's high-risk third country list (due to the identified high ML/TF risk of these jurisdictions) and
- risk areas identified by NPOs. [17]

After extensive research, questionnaires were distributed to all NPOs that potentially fall into one of the two risk groups. The evaluation of the questionnaires revealed a potential threat for 80 of the total of around 135,000 NPOs in the country. This corresponds to around 0.06% of the entire Austrian NPO sector.

The background to this is that the large Austrian NPOs perform a very broad range of tasks, ranging from social counselling, care for the elderly, emergency services and hospitals in Austria to development projects and emergency humanitarian aid in third countries. Conversely, some smaller NPOs devote themselves entirely to development and humanitarian aid in third countries.

The following overview is a summary of the 2023 and 2024 NPO risk surveys and includes those countries that are on the grey/black list or for which NPOs have identified terrorist financing risks. This is not an overall list of the activities of Austrian NPOs, but rather a presentation of the threat scenarios. The regions are listed in descending order of threat intensity.

[17] The particular risks in relation to countries with the influence of terrorist groups are exacerbated by the fact that these are countries - especially Lebanon, Yemen and Gaza - where there is de facto no willingness for judicial cooperation.

Middle East:

The Middle East is the region with the highest identified threat level in comparison. NPOs identified increased threats in the following countries: Iraq, Lebanon, Yemen, Afghanistan, Israel/Palestine and Syria. Terrorist financing risks exist through the direct/indirect diversion of aid funds, theft, recruitment activities/infiltration, expropriation and attempts to influence tenders. There are particular risks in jurisdictions (Lebanon, Gaza, Yemen) where terrorist groups have far-reaching influence. Many Austrian NPOs support ethnic/religious minorities that are themselves targeted by terrorist groups (often, but not exclusively, Christian minorities). While this exposes them to physical risks, it reduces the threat of infiltration by terrorist groups.

Africa:

Austrian NPOs are mainly active in Kenya, Tanzania, Burkina Faso and Mozambique. The highest identified terrorist financing risks exist for Mozambique (especially Cabo Delgado) and Burkina Faso. The identified terrorist financing risks include diversion, kidnapping, extortion and recruitment activities/infiltration attempts. In some countries with a territorial presence of terrorist groups (Somalia, Nigeria), NPOs are active under the protection of the army, police or private security forces. Many Austrian NPOs support ethnic/religious minorities that are themselves targeted by terrorist groups (often, but not exclusively, Christian minorities). While this exposes them to physical risks, it reduces the threat of infiltration by terrorist groups.

South and Southeast Asia:

Austrian NPOs are mainly active in India, Pakistan, the Philippines and Vietnam. The highest identified terrorist financing risks exist for Pakistan (especially Balochistan and Khyber Pakhtunkhwa) and the Philippines (Mindanao). Risks from terrorist groups consist primarily of violence against the civilian population, particularly ethnic/religious minorities. The identified terrorist financing risks include diversion and extortion. Many Austrian NPOs support ethnic/religious minorities that are themselves targeted by terrorist groups (often, but not exclusively, Christian minorities). While this exposes them to physical risks, it reduces the threat of infiltration by terrorist groups.

Latin America:

Latin America has the lowest identified risk scenarios in comparison. Austrian NPOs are mainly affected by two potential threat scenarios:

- In Ecuador, Brazil (Bahia), Colombia (Guaviare and others with the Disidencia; Ejército de Liberación Nacional (ELN), Ejército Popular de Liberación (EPL), FARC dissidents) and Peru (Sendero Luminoso), paramilitary groups and (former) guerrilla groups are particularly active in border regions. Identified terrorist financing risks exist primarily in infiltration for recruitment purposes.
- In Venezuela, Hezbollah is involved in drug trafficking and money laundering in order to generate funds that are relevant to terrorist financing. Indirect terrorist financing risks may arise for NPOs (e.g. business with Hezbollah-controlled companies).

Contextual factors:

In addition to the countries listed by the FATF and the European Commission, NPOs identified a number of other countries. These often, but not always, had a generally poor security situation. No NPOs reported risks in connection with projects in Austria. This assessment is in line with the threat analysis on terrorism financing in the National Risk Assessment 2025.

In conflict zones, NPOs are confronted with acute physical risks, including from terrorist groups. Identified terrorist financing risks did not occur in isolation, but were part of a range of other identified physical risks (often in combination with terrorist attacks and armed conflicts) and financial risks (primarily corruption).

NPOs counter the identified risks in different ways. Smaller NPOs with a presence in risk areas tend to withdraw from the affected region and sometimes from the affected country altogether when physical risks are identified, which are generally associated with increased terrorist financing risks. This risk limitation reduces the overall threats to which they are exposed. Larger, professionally structured NPOs remain on the ground even if the local security situation deteriorates and the associated terrorist financing risks increase. It can be observed that these NPOs utilise a wide range of risk mitigation measures to manage their physical and financial risks.

This dynamic is reflected in the individual risk assessments. While Austrian NPOs identified a number of threats from terrorist groups in the countries in which they operate, only a relative minority in these countries were actually active in those specific areas particularly affected by terrorist threats.

The financial flows mainly go to larger, professionally organised NPOs that carry out numerous projects. Due to their higher profile and better access to funding from institutional donors (in particular the Austrian Development Agency and the European Commission's ECHO programme), they provide the vast majority of funding in areas with an active terrorist threat.

<u>Conclusion</u>: In summary, the threat is categorised in different ways:

In general, the threat to the NPO sector can be categorised as low.
For those NPOs (approx. 0.06% of the sector),

- **have identified terrorist financing risks in certain project areas or**
- **operate in countries on the FATF lists or the European Commission's high-risk third country list**

the threat is categorised as high to very high. This categorisation only applies to the NPO project area, which falls under the two identified risk areas. For the other project areas, the threat is categorised as low.

<u>Sectoral risks</u>

In contrast to those associations that adhere to the legal requirements and the risk of being misused for terrorism financing, those NPOs that

- can be used for terrorism financing,

- were set up specifically for the purpose of terrorism financing,
- Organised crime, terrorism and therefore also the

Accept terrorism financing.

As already mentioned in the organisational article, it is primarily associations that are affected. The first two categories include donation and aid organisations, which may also attempt to obtain seals of approval under false pretences.

An increased threat is posed in particular by those NPOs (but deliberately misused) that do not limit their presence and activities exclusively to the domestic market, but are - at least partially - financed from abroad (EU and/or third countries), or (also) receive donations from abroad and then subsequently forward them abroad (EU and/or third countries).

With such charitable organisations, there is a risk that funds or other donations in the form of collections of assets such as clothing, food or equipment will not go to those actually in need, but will be made available in whole or in part terrorist or terrorism-related organisations. In doing so, no or no suitable control mechanisms are deliberately set up during distribution or the control mechanisms are circumvented. As a result, the distribution of donations of goods and money is not or only inadequately monitored, which means that uncontrolled distribution of goods - and thus a transfer to terrorist organisations/persons - can take place.

The third category includes so-called OMCG (outlaw motor cycle gangs), i.e. organised motorbike gangs that have constituted themselves as associations. They therefore deserve special attention in connection with terrorism financing, as they financed not only through membership fees, the sale of supporter clothing, work in the security industry, the red light sector or in tattoo shops, but also by criminal offences and pose a threat to public safety through their radical extremist appearances.

It cannot be completely ruled out that other NPOs - not listed here - may also be established or exploited for the financing of terrorism, in particular through the provision of infrastructure or training. However, the threat in this regard can be categorised as low.

<u>Conclusion</u>: To summarise, the sectoral threat in relation to the NPO sector as a whole can be classified as present but low.

Vulnerability

<u>Organisational risks</u>

In the summarised scenarios of the Supranational Risk Assessment, the vulnerability of NPOs that collect or distribute donations to misuse for terrorist activities was classified as **medium** risk. NPOs that receive institutional funding, including from the EU or from Member States responsible for the management of EU funds, are considered to have a **low** vulnerability to terrorism financing. As a result, the national vulnerability is to be derived.

(a) Risk potential:
Most of the activities of Austrian NPOs take place in Austria. Only a small part of the sector has an international presence, and an even smaller part of this in countries that are exposed to increased terrorist financing risks (approx. 0.06% of the sector based on the risk survey, see calculations above). The risk potential can therefore be categorised as low overall. As even relatively small sums can be used for terrorism, the risk potential in the small segment of the sector with activities in identified risk areas can be categorised as high.

(b) Risk awareness:
The risk-mitigating measures of Austrian NPOs were surveyed by the BMF in 2023 and 2024. The catalogue included various measures in the areas of organisational structure and governance, documentation, finance, external audits, partner organisations and risk management in the area of terrorism financing. In addition to specific measures such as risk assessments in relation to terrorism financing or sanction screenings, other risk management techniques such as control structures, partner assessments or documentation and reporting obligations that reduce financial risks and, indirectly, terrorism financing risks were recorded.

The evaluation of the risk mitigation measures was not a static tick-the-box approach. The risk mitigation measures were assessed in terms of whether they addressed the identified risks - the pure quantity of measures implemented was not the decisive factor. Analysing the questionnaires revealed a differentiation within the sector.

NPOs that carry the Austrian Donation Seal of Quality, have ADA or ECHO accreditation or are members of the Coordination Centre of the Austrian Bishops' Conference implemented the overwhelming majority of the measures. The explanations of the measures showed a very good understanding of physical and financial risks and a well-developed understanding of terrorist financing risks.

NPOs outside of these networks also generally apply several of the aforementioned risk minimisation measures, particularly with regard to the general control of financial flows. The scope and intensity of the measures taken generally increase with the size of the NPOs. However, it can also be observed that some small NPOs can demonstrate very solid risk minimisation measures. These include, in particular, NPOs with employees from the financial sector who have the relevant prior knowledge.

The results of the risk surveys will be confirmed by a survey of the members of the umbrella organisations AG Globale Verantwortung (Global Responsibility) and KOO in summer 2024:

- 85.2% of organisations stated that their awareness of the risk that their organisation or their partner organisations could be misused for terrorism financing has increased over the past 5 years.
- 92.6% of organisations stated that they had tightened their risk management measures in one or more areas in the past 5 years.

(c) Legal framework and supervision/governance:
The NPO sector is subject to a range of government measures, external and independent control mechanisms and self-regulatory initiatives.

1. Government measures

Examination of the deductibility of donations:
As voluntary donations, donations are generally not tax-deductible. However, by law, donations to the organisations listed in article 4a EStG are deductible as business expenses (if made from business assets) or as special expenses (if made from private assets) up to a limited amount. Since 1 January 2024, the option to deduct donations has been open to all charitable, benevolent, scientific and adult education purposes.

The corporate body must apply for the granting of preferential treatment for donations using an official electronic form. This must be submitted by a professional party representative in accordance with the Wirtschaftstreuhandberufsgesetz 2017 (WTBG 2017). The applicable legal basis of the corporation must be enclosed with the application. In order to maintain the preferential treatment of donations, the fulfilment of the requirements for the preferential treatment of donations must be reported annually to the Austrian tax office by professional party representatives in accordance with the WTBG 2017.

In the case of corporations that are subject to the obligation to have their annual financial statements audited by an auditor in accordance with the law or their articles of association, the fulfilment of the requirements and compliance with the applicable accounting regulations must also be confirmed by an auditor in accordance with articles 268 et seq. of the Austrian Commercial Code (UGB) when the application is submitted and annually thereafter.

The Austrian tax office must issue an official notice stating that the legal requirements for the initial granting of preferential treatment for donations have been met and include the corporation in a list of beneficiaries of donations to be maintained by the Austrian tax office. In this list, the date on which the donation favour was granted must be published. The list must be published on the website of the Federal Ministry of Finance.

If the requirements are no longer met or if the timely reports are not submitted despite a reasonable grace period being set, the donation authorisation must be revoked by official notice.

Of the largest 100 NPOs - which account for 74% of all donations to civil society organisations - only 6 are not donation-favoured. However, these organisations also require an auditor under other legislation (e.g. Association Act, Private Foundation Act, Federal Foundation and Fund Act): Association Act, Private Foundation Act, Federal Foundation and Fund Act).

In addition, a further € 43 million (around 5% of all donations to NGOs) to smaller, non-auditable organisations (less than 1 million donations) are also audited as part of the donation tax

concessions. Depending on their size, audits are prescribed for non-profit organisations in the Austrian Association Act, Private Foundation Act, Federal Foundation Act and Fund Act. Federal and provincial foundations have their own supervisory authority in the form of the provincial foundation authorities (and in certain cases also the Finanzprokuratur).

As described above, donations are concentrated in large NPOs that are characterised by professional structures and the implementation of numerous risk-mitigating measures. 94% of the donations made by all civil society structures are audited by a chartered accountant who certifies the raising and use of funds, and 75% of all donations are subject to an in-depth audit for the Austrian Donation Seal of Quality.

Donation volume and audits in Austria 2022					
	Donations		**Mandatory audits**	**Auditors**	**Vountary audits**
NGOs	€ 920.000.000	83%	€ 867.000.000	Public accountants (Wirtschaftsprüfer)	€ 691.870.00
Public entities	€ 160.000.000	15%	€ 160.000.000	Courts of Auditors and others	Not possible
Churches	€ 23.000.000	2%	€ 23.000.000	Federal Chancellery - Office of Religious Affairs	Not possible
Sum	**€ 1.103.000.000**		**€ 1.050.000.000**		**€ 691.870.00**
NGOs only	100%		94%		75%
not audited			€ 53.000.000		€ 228.130.00

Comparison of the total volume of donations against mandatory audits as part of the tax deductibility and the audits carried out by the Austrian Donation Seal of Approval.

Risk surveys by the BMF:

In 2023 and 2024, the Federal Ministry of Finance conducted a survey of potential threats and risk management measures in the Austrian NPO sector. The questionnaires are usually completed or forwarded by the management level of the NPOs and are already used to raise awareness in this way. Around 450 questionnaires were sent out in 2023 and around 350 in 2024 (a lower number due to better knowledge of which NPOs fall within the scope). Many NPOs have already dealt intensively with their own terrorist financing risk and the questionnaires led to an in-depth examination of the topic at all NPOs.

Risk-based audits by the Tax Authority Austria:

Based on the risk survey, the association-specific audit quota of the Austrian tax office is partially reallocated in order to carry out random audits of NPOs with an identified risk. These audits focus on cases with very high and high risk. They relate to the fulfilment of legal requirements with regard to statutes and financial management. The auditors take into account an internal document with terrorism financing red flags.

Outreach by the BMF:

The BMF offers all NPOs the opportunity to receive feedback on the submitted questionnaires free of charge. The Federal Ministry of Finance has also set up its own NPO mailbox for all questions relating to the prevention of terrorism financing and provides detailed information on its website on how NPOs can protect themselves from being misused for terrorist purposes. As part of the Public Private Partnership with the NPO sector (PPP NPOs) established in 2023, the Federal Ministry of Finance regularly exchanges information with umbrella organisations and

interest groups in the NPO sector and provides information on activities, measures and legal requirements for the prevention of terrorism financing.

The BMF regularly organises lectures for the NPO sector, for example a lecture on "Foreign currency transfers to third countries" or a workshop on "Country risk analysis".

The PPP NPOs has introduced an innovative new risk sensitisation tool. PPP NPOs members and NPOs with specific country expertise are working together to produce country fact sheets on TF risks for NPOs. They combine information from official sources (FATF reports, national risk assessments, sectoral risk assessments) with reports from renowned research institutions and input from NPOs operating in the respective country.

This cooperation ensures that the NPOs are involved from the outset and contribute their practical experience. The first country risk report on Kenya has already been finalised and work on further fact sheets is underway.

The BMF also provides information on the risks and risk-minimising measures in the NPO sector as part of the National Coordination Committee and various public-private partnerships with obliged entities. This provides authorities and obliged entities with up-to-date information on the NPO sector.

2. External, independent control mechanisms

Accreditation by the Austrian Development Agency (ADA)

In order to be able to implement ADA-funded projects in the humanitarian sector or Nexus projects, NPOs must be accredited by ADA in advance. The prerequisite is the fulfilment of strict quality standards, among other things, applicant organisations must provide evidence of internal processes and control systems to prevent fraud, corruption, bribery, money laundering, terrorism financing and other forms of abuse.

EU Humanitarian Partnership Certificate 2021-2027 (DG ECHO)

Similar to ADA, NPOs can pre-qualify as implementation partners for humanitarian measures with DG ECHO, which reports to the European Commission. In order to receive the EU Humanitarian Partnership Certificate from DG ECHO, the applicant organisations must, among other things, fulfil quality criteria that are explicitly aimed at preventing terrorism financing and money laundering.[18]

Other measures

[18] DG ECHO (n.d.): Terms of Reference for the ex-ante assessment. Retrieved from: https://www.dgecho-partners-helpdesk.eu/download/referencedocumentfile/91

In addition to the measures mentioned above, other funding organisations also check the proper use of funds. For example, there is a statutory audit obligation for larger organisations (annual donations of EUR 1 million or more) under the law on associations. The ADA carries out a standardised partner assessment for funding of EUR 100,000 or more and other public funding bodies (e.g. federal states, ministries, EU/INTPA) also have their own audit procedures for their funding recipients.

3. Self-regulatory measures

On the one hand, NPOs co-operate with each other in various associations and, on the other hand, compete for donations. The appropriate use of donations is a central argument in fundraising. As a rule, NPOs prominently emphasise the tax-deductibility of donations, the donation seal of approval or other measures for the appropriate use of funds.

The Austrian Donation Seal of Quality

The Austrian Donation Seal of Quality is awarded by the Chamber of Tax Consultants and Auditors (KSW). It proves that a donation organisation handles the funds entrusted to it carefully and responsibly and ensures that donations are used for the intended purpose and in an economical manner.

All donation seal of approval organisations voluntarily undertake to fulfil the comprehensive criteria of the Austrian Donation Seal of Quality and are audited once a year by an independent tax consultant or auditor - obliged entities under the WTBG. Every OSGS audit includes explicit risk-minimising measures with regard to money laundering and terrorism financing.

The Coordination Centre of the Austrian Bishops' Conference ("KOO"):

The Coordination Office of the Austrian Bishops' Conference represents the interests of Catholic institutions and organisations in Austria that are involved in development cooperation, domestic development work or missionary cooperation and is responsible for networking, coordination and quality assurance.

The (currently 35) members of the KOO interest group follow a set of common rules and standards and are subject to episcopal supervision. In the event of violations and misconduct, the Austrian Bishops' Conference can impose sanctions up to and including expulsion from the organisation.

The Coordination Office of the Austrian Bishops' Conference operates a fraud warning system among its members, with which fraudulent project applications are shared in the network, centrally documented and analysed.

Training within the NPO sector:

Umbrella organisations and interest groups in the NPO sector contribute with numerous events and activities to informing and sensitising the sector to terrorist financing risks and to measures that NPOs can take to protect themselves against these risks.

The motto of the 2024 Austrian Donation Seal of Approval Forum was "Prevention instead of reaction - money laundering, terrorism financing and the influence of political debates on NPOs". Members of the KSW, NPOs and representatives of the Federal Ministry of Finance addressed the question of how NPOs can protect themselves against unjustified accusations of money laundering and terrorism financing.

The **Fundraising Association Austria** organises at least 2-3 seminars a year on the subject of "Law and Taxes". The basic principles of the topic are also part of the content. In the more comprehensive training programme for fundraisers, the two-semester diploma course "Fundraising Operations & Management", the topic is dealt with in detail.

AG Global Responsibility, the umbrella organisation of development and humanitarian NPOs in Austria, has organised a total of 6 events with expert input for its member organisations on the topic of counter-terrorism measures since 2021. Among other things, participants were trained in the practical handling of sanctions lists, the management of terrorist financing risks and the prevention of corruption. In addition, the Global Responsibility Working Group conducted several surveys among its members on the topic and contributes to raising awareness in the sector with ongoing mailings and information.

In addition, in the first half of 2024, the Global Responsibility Working Group, together with the Coordination Office of the Austrian Bishops' Conference, organised a series of events on challenges and solutions in international payment transactions for NPOs, which also served to raise awareness of terrorist financing risks.

Since 2021, the **Coordination Office of the Austrian Bishops' Conference** has organised a total of 4 events on the topic of "Prevention of money laundering and terrorism financing". Two events are organised each year to address different quality assurance issues in international project work, including partner assessments, fraud attempts and payment instruments. Furthermore, the Coordination Office of the Austrian Bishops' Conference carried out several surveys among its members on money transfers in conflict and risk regions during the period mentioned and contributes to information and awareness-raising among its members with ongoing mailings and a central fraud warning system.

International financial flows and risk mitigation measures

In 2021, Austrian NPOs spent private funds totalling € 172 million on development and humanitarian aid in developing countries (over 90%) and on administration and educational and public relations work in Austria (less than 10%). Developing countries are those listed in the OECD Development Assistance Committee's list of recipient countries. This includes countries listed by

the European Commission or the Financial Action Task Force, but also other countries without increased risk.

- 98.3% of the funds were used by organisations that receive donations and are therefore audited annually by independent, external auditors.
- Of the organisations that do not receive donations, at least a further third are nevertheless audited. This increases the proportion of funds implemented by audited organisations to 98.9%.
- 83.4% of the funds were used by organisations that bear the Austrian Donation Seal of Approval and are audited annually by external, independent auditors on the basis of strict quality criteria - including criteria on terrorism financing and money laundering.
- 38.6% of the funds were implemented by organisations that are accredited as implementation partners with the ADA and have undergone a strict qualification process - including a review of criteria relating to terrorism financing and money laundering.
- 25.7% of the funds were implemented by organisations that are certified as DG ECHO implementation partners and have undergone a strict DG ECHO audit procedure - including criteria relating to terrorism financing and money laundering.
- 89.0% of the funds were used by organisations that have either undergone the annual audit procedure for the donation seal of approval or the procedure for obtaining ADA accreditation or ECHO certification and have thus been checked by one or more external, independent bodies for compliance with criteria on terrorism financing and money laundering. In practice, ADA accreditation and ECHO certification tend to be designed for large, humanitarian NPOs.

	Private Zuschüsse 2021 (in €)	**Anteil an Gesamt**
Gesamt	172.002.728	
davon umgesetzt von		
spendenbegünstigten NPOs	169.041.392	98,3%
wirtschaftsgeprüften NPOs	170.081.841	98,9%
OSGS-zertifizierten NPOs	143.415.198	83,4%
ADA-akkreditierten NPOs	66.379.513	38,6%
ECHO-zertifizierten NPOs	44.209.726	25,7%
OSGS-zertifizierten, ADA-akkreditierten oder ECHO-zertifizierten NPOs	153.051.757	89,0%

Source: AG Global Responsibility based on data from ADA, BMF, DG ECHO, KOO and KSW

Overall, it can be seen that 98.9% of international project funds are managed by NPOs that are subject to at least one and often several external audits. 89.0% of all funds are implemented by NPOs that are subject to one or even several audits by external, independent bodies (KSW, ADA, DG ECHO), which include criteria on money laundering and terrorism financing.

All of the above measures have a risk-minimising effect. The Austrian Donation Seal of Quality, ADA accreditation and ECHO certification have a particularly sustainable risk-reducing effect due to their comprehensive scope of testing and regular recertification measures by external bodies. The evaluation of the risk survey questionnaires also showed that NPOs that have one or more of the three certifications have a very high level of risk awareness and have set up comprehensive risk management systems. Their vulnerability can therefore be categorised as low. NPOs outside of these networks generally apply several of the aforementioned risk minimisation measures, in particular measures for the appropriate use of financial resources. The scope and intensity of the measures taken generally increase with the size of the NPO. However, it can also be observed that some small NPOs have very solid risk minimisation measures. Overall, the vulnerability of NPOs outside of these networks can be categorised as medium to high.

Human and financial resources: 1.5 FTEs are allocated to strategic tasks, outreach and risk assessment at the Federal Ministry of Finance. 6 specially trained auditors from the Austrian tax office carry out the audit activities.

<u>Conclusion</u>: In general, the vulnerability of NPOs to being misused for the purposes of terrorism financing must be categorised in different ways.

This categorisation only applies to NPOs with identified risk factors (approx. 0.06% of the sector)[19]. However, many of the control measures mentioned are widespread in the NPO sector.

The vulnerability of NPOs to being misused for terrorism financing purposes is low for NPOs that

- **the Austrian Donation Seal of Approval,**
- **ADA accreditation**
- **and/or have ECHO certification.**

The vulnerability of NPOs outside these networks can be categorised as medium to high.[20]

<u>Sectoral vulnerability</u>

The legal entities used for non-profit activities (associations, private foundations, as well as stock corporations and limited liability companies) were assessed with a medium legal form-specific risk (cooperatives with a low risk).

[19] NPOs with projects in countries listed by the European Commission or the Financial Action Task Force, as well as projects where NPOs have identified terrorist financing risks.

[20] This assessment represents an average value. The risk surveys found NPOs that also had low vulnerability due to extensive control systems. A very small number of NPOs had high to very high vulnerability due to weak control systems.

For the NPO sector, it should be noted that the control mechanisms described above (mandatory audits above a certain amount and the funding organisations' own audits) apply. In addition, the donation behaviour of the population tends towards established NPOs that are subject to control mechanisms such as the deductibility of donations and the Austrian Donation Seal of Quality. As already described, the volume of donations is increasingly concentrated on large NPOs that are characterised by professional structures and the implementation of numerous risk-minimising measures. 94% of donations from all civil society structures are audited by a chartered accountant who certifies the raising and use of funds, and 75% of all donations are subject to the in-depth audit for the Austrian Donation Seal of Approval. 98.9% of international project funds are managed by NPOs, which are subject to at least one and often several external audits.

It is therefore possible to simply set up an association, for example, but legal and factual obstacles make it difficult to misuse an NPO to realise larger sums.

Conclusion: To summarise, the vulnerability of the NPO sector to targeted terrorism financing by individual NPOs can be classified as low to medium.

Total risk

Organisational risk:

In the summarised scenarios of the Supranational Risk Assessment, NPOs that collect or distribute donations were classified as **medium** risk for misuse for terrorist activities. NPOs that receive institutional funding, including from the EU or from Member States responsible for managing EU funds, are considered to have a **low** vulnerability to terrorism financing. Subsequently, the national risk is to be derived.

In summary, this results in a differentiated categorisation of the overall risk:

In general, the risk for the NPO sector of being misused for terrorism financing purposes can be classified as low.

The risk of those NPOs with projects in identified risk areas (approx. 0.06% of the sector)[21] being misused for terrorism financing purposes is medium if they

- **the Austrian Donation Seal of Approval,**
- **ADA accreditation**
- **and/or have ECHO certification.**

[21] Projects in countries listed by the European Commission or the Financial Action Task Force, as well as projects where NPOs have identified terrorist financing risks.

The risk of NPOs outside these networks in projects in identified risk areas[22] can be categorised as medium to high.[23]

This categorisation only applies to the NPO project area that falls under the two identified risk areas. For the other project areas, the risk is categorised as low.

Sectoral risk:

To summarise, the NPO sector's risk of targeted terrorism financing by individual NPOs can be classified as low to medium.

Recommendations

The recommendations are aimed at authorities and include suggestions on how to improve the prevention of money laundering and terrorism financing. Due to the density of state control, external and independent control mechanisms and self-regulatory measures in the sector, no legal changes are currently required.

- Ensuring and improving data quality
- Carrying out the risk survey
- Continuation of government control measures
- Training and presentations for the sector

[22] Projects in countries listed by the European Commission or the Financial Action Task Force, as well as projects where NPOs have identified terrorist financing risks.

[23] This assessment represents an average value. The risk surveys revealed NPOs that also have a medium risk due to extensive control systems. A very small number of NPOs have a high to very high risk due to weak control systems.

Federal Ministry of Finance
Johannesgasse 5, 1010 Vienna
+43 1 514 33-0
email@bmf.gv.at
bmf.gv.at