Bundesministerium
Finanzen

National Risk Assessment of money laundering and terrorist financing

Vienna, 2021

Imprint
Media owner, publisher and editor:
Federal Ministry of Finance, Johannesgasse 5, 1010 Vienna
Vienna, 2021. Version of: 11. Mai 2021

Feedback: Please send any observations you may have on this publication to email@bmf.gv.at.

Foreword

Dear Ladies and Gentlemen,

Money laundering and terrorist financing have remained extremely present challenges in recent years. The importance of effective preventive measures for protecting the financial markets and the national economy as a whole from incriminated funds has consistently been evident. Effective control systems also strengthen the reputation of companies and thus contribute to Austria's competitiveness as a business location.

A core component of the international and European standards for combating money laundering is the risk-based approach, which characterises the measures for preventing money laundering and terrorist financing. The most important element of the risk-based approach is the preparation of risk assessments at supranational and national levels as well as for the economic sectors and companies concerned.

This National Risk Assessment thus represents an important foundation for the measures for the prevention of money laundering and terrorist financing. It identifies the risks to the sectors concerned by analysing the prevailing threats and vulnerabilities and is intended to enable authorities and obliged entities to utilise their resources in a targeted manner and to take effective preventive action. This National Risk Assessment is the joint outcome document of all the authorities involved in preventing and combating money laundering and terrorist financing in Austria. It was drafted on the basis of detailed sector risk assessments.

The individual assessments reveal a diverse risk landscape. Risks of money laundering and terrorist financing differ in relation to individual products and services, both within the same sector and between sectors.

The National Risk Assessment is also intended to contribute to a better understanding of risk by all the authorities concerned and by the private sector and thus to lead to a more effective overall fight against money laundering and terrorist financing in Austria. The Federal Ministry of Finance is committed to implementing international and European standards for combating money laundering and to the continuing further development of those standards along with its European and international partners.

Mag. Harald Waiglein, MSc.
Director General of DG III – the Directorate General for Economic Policy, Financial Markets and Customs Duties

Table of contents

Introduction

1. Objectives of the National Risk Assessment

The **basis for all measures** for the prevention of money laundering and terrorist financing by public 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 this National Risk Assessment is to create such a basis.

Pursuant to Art. 3 para. 3 of the Financial Markets Anti-Money Laundering Act [German acronym: FM-GwG] and **Art. 7 para. 4 of the 5th Anti-Money Laundering Directive [AMLD],** the National Risk Assessment serves the following purposes:

- **Improvement of the regime** for combating money laundering and terrorist financing, in particular by **identifying any areas** where obliged entities are required to apply **enhanced measures,** and by **recommending the measures to be taken.**
- **Identification of sectors or areas** of **low** or **increased risk** of money laundering and terrorist financing.
- **Identification of** money laundering and terrorist financing **risks** in relation to the development of **new products** and **business practices,** including **new delivery channels** and the use of **new or developing technologies** both for **new** as well as for **existing products**.
- **Allocation of resources** and **prioritisation** to combat money laundering and terrorist financing.
- **Ensuring** that appropriate rules are drawn up **for each sector or area** commensurate with the risks of money laundering and terrorist financing.
- Swiftly providing **obliged entities with appropriate information** to assist them in carrying out their own money laundering and terrorist financing risk assessments.
- Reporting on the **institutional structure** and **main features of the systems** for combating money laundering and terrorist financing in Austria*, inter alia* in relation to the Financial Intelligence Unit (FIU), tax authorities and public prosecutors, as well as the human and financial resources allocated, provided that such information is available.
- Reporting on **national efforts and resources** (in terms of human resources and funding) that are made available for combating money laundering and terrorist financing.

The Federal Ministries of Finance, of Justice, of the Interior, for Digital and Economic Affairs, for European and Foreign Affairs, as well as the Financial Market Authority (FMA) and the Oesterreichische Nationalbank are required to take **appropriate measures** within the scope of their respective remits **to achieve these purposes**.

2. Preparation for the National Risk Assessment

The **first Austrian National Risk Assessment for Austria (NRA I)** dates from **April 2015.** Since then, the European and international legislative framework has been constantly evolving. The Financial Action Task Force's (FATF) country assessment of Austria in 2015 and 2016 resulted in new recommendations for implementing the National Risk Assessment. **The risk situation has also been constantly evolving** and the **substantive laws have been extended** to apply to new obliged entities. An update is therefore appropriate.

The starting point for the National Risk Assessment is the **National Coordinating Committee** established at the Federal Ministry of Finance **to develop measures and strategies for the prevention of money laundering and terrorist financing**. This body is composed of all relevant authorities.

Pursuant to **Art. 3 para. 2 FM-GWG,** the Coordinating Committee is required to draw up and keep up to date a National Risk Assessment for the development of measures and strategies for the prevention of money laundering and terrorist financing. The **basis of the National Risk Assessment** is to consist of the **contributions of the members,** which they must prepare in relation to their respective remits.

The preparation process proceeded in three stages.

1) Based on a **common template and methodology,** the members drew up a **first draft of their sector risk assessments**. These are **outcome documents** presenting the conclusions and results of **detailed preliminary assessments**. This approach and the corresponding compactness of the contributions take into account **the FATF's recommendation** from the last country assessment of Austria.
2) The first drafts were sent to the **Federal Ministry of the Interior** for **comparison with operational findings.** In parallel, the relevant **representatives of the private sector** received the draft report for comment.
3) The **final drafts were prepared** and consolidated into one overall document, **taking into account feedback** from the Federal Ministry of the Interior and from the private sector.

3. Methodology

The **updated National Risk Assessment (NRA II)** is to take into account the recommendations of the 2016 FATF country report, as well as the provisions of the 4th and 5th AMLD.

The sector risk assessments are based on the **methodology of the Supranational Risk Assessment (SNRA)**, which is to be prepared by the European Commission according to Art. 6 para. 1 of the 5th AMLD. A comprehensive presentation of the underlying methodology is contained in the Staff Working Document (SWD) of the SNRA 2017, p. 233 *et seq*. The most up-to-date SNRA, whose risk assessment were taken into account by the sector risk assessments, was published in 2019.

The central points of this methodological approach are briefly outlined below. The **threat** and **vulnerability** for money laundering and terrorist financing are each assigned **a value** corresponding to the SNRA values 1 - 4 (lowly significant/moderately significant/significant/very significant). The **classification of threat and vulnerability** follows the description of the SWD 2017, p. 248 *et seq*. Quantitative figures and findings obtained in the course of supervisory activities serve as the source of the data. The existing risk-mitigating measures are subsequently described.

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

As with the SNRA methodology, the National Risk Assessment assumes that **vulnerability** has a **stronger effect on overall risk** than does threat, and that it should therefore be weighted more heavily.

Finally, the sector risk assessments formulate **recommendations** on the basis of the findings. As the National Risk Assessment is a document from a public authority, the recommendations are only addressed to **public authorities.** The competent authorities remain free to formulate further measures in relation to their obliged entities on the basis of the findings made in the course of their supervisory activities.

Predicate offences to money laundering

Analysis of predicate offences to money laundering

General information

The term "predicate offence"

This article examines the offence of money laundering (Art. 165 of the Austrian Criminal Code [German acronym: StGB]) from the perspective of predicate offences to money laundering and based on several sources, it describes predicate offences which are particularly common in connection with money laundering and whose risk of being committed is therefore particularly high.

Pursuant to Art. 165 para. 1 StGB, any person who conceals or disguises the origin of any proceeds originating from certain criminal offences punishable by imprisonment for up to three years. A central function of criminalising this action, which is defined as "money laundering", is to render the use of illegally obtained proceeds more difficult by also penalising the concealment of such assets or the disguising of their origin.

Money laundering is what is known as a criminal offence after the fact. This means that for it to be a punishable offence (with the exception of Art. 165 para. 3 StGB), proof of **certain predicate offences is also required**. The list of predicate offences under Art. 165 para. 1 StGB has, in the past, been continually expanded such that today, laundering of any proceeds originating from acts punishable by imprisonment for more than one year or from offences under Art. 223, 229, 289, 293, 295 StGB or Art. 27 or 30 of the Narcotic Substances Act [German acronym: SMG] is a punishable offence.

Money laundering is a punishable offence, irrespective of whether it is committed by the same perpetrators as the predicate offence (which is known as self-laundering) or by third parties. However, in contrast to self-launderers, third parties are not only liable to prosecution pursuant to Art. 165 para. 2 StGB if they conceal or disguise the origin of proceeds susceptible to money laundering, but also if they knowingly acquire, hold, invest, administer, convert, exploit or transfer such asset components.

Finally, pursuant to Art. 165 para. 3 StGB, any person who knowingly acquires, holds, invests, administers, etc. asset components subject to the control of a criminal organisation or a terrorist group is also liable to prosecution. Because of the high criminal energy of such groups and the dangers posed by them, the existence of a predicate offence for money laundering is not relevant to this type of offence.

Source of data for the risk assessment

The A-FIU (Austrian Financial Intelligence Unit) is part of the security authorities and therefore bases the following analysis on the following sources: First, the A-FIU, as the central financial intelligence unit for money laundering, receives suspicious transaction reports (STRs) from the professional groups subject to reporting obligations. From the facts presented in the suspicious transaction reports, which suggest certain predicate offences, it can

extrapolate the risk of such offences being committed (Figure 1). Second, the assessment is based on data from the crime statistics for the years 2018 to 2020 (Figure 2). From these, it can be determined which offences were most frequently investigated in connection with the basic offence of money laundering (but not which ones led to convictions!). These statistics, therefore, also show offences that do not meet the definition of a "predicate offence" within the meaning of Art. 165 StGB, e.g. because they are not punishable by imprisonment for more than one year (this includes, for example, simple theft).

Furthermore, the following analysis also takes into account fields of criminal activity for which the A-FIU receives hardly any suspicious transaction reports, but for which we can presume a high number of unreported cases. These are mainly drug-related offences and offences in the field of organised crime.

Data concerning predicate offences that other agencies are responsible for investigating are not described; these include predicate offences related to tax offences and corruption as well as terrorist financing.

The following statistics of suspicious transaction reports and data from the police crime statistics show the offences most commonly connected with money laundering.

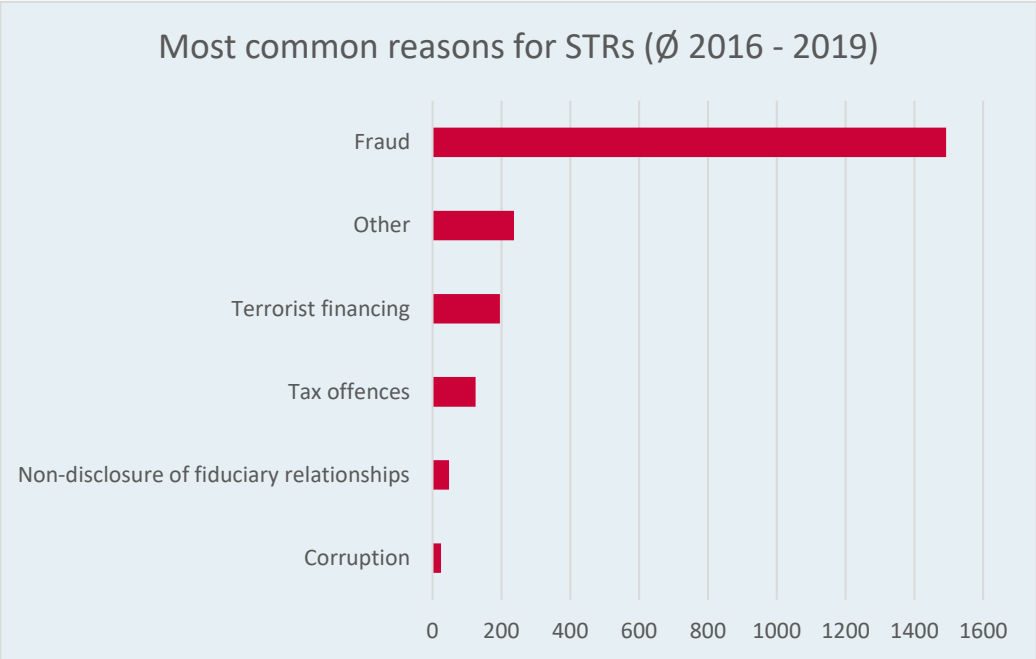

Figure 1

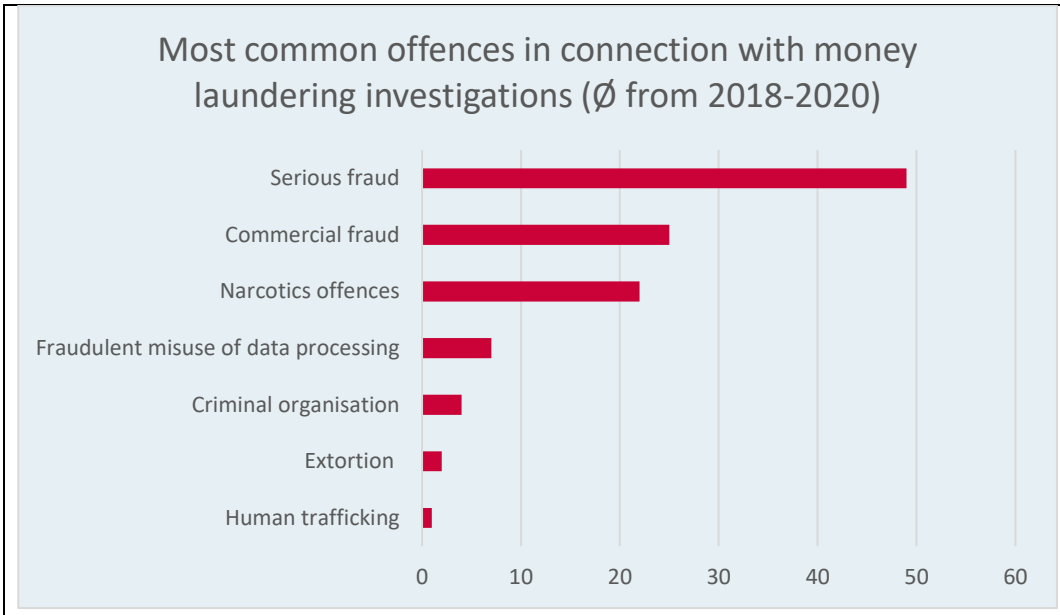

Figure 2

Most common predicate offences to money laundering: Fraud

According to police crime statistics, in investigations of money laundering over the last three years, an average of 49 cases were suspected to be linked to serious fraud (Art. 147 StGB). A link with commercial fraud (Art. 148 StGB) was established in an average of 26 cases over the same period, and fraudulent misuse of data processing (Art. 148a StGB) in seven cases.

The frequency of fraud offences is also consistent with findings extrapolated by the A-FIU from the suspicious transaction reports it receives, since suspicious transaction reports relating to money laundering are most often filed due to suspicion of fraudulent activities. Financial and credit institutions have long experience with this criminal phenomenon and therefore recognise the practices that suggest acts of fraud.

Fraud takes place predominantly on the Internet now. Due to the democratisation of the Internet, almost everyone has internet access today, and more and more aspects of everyday life are conducted in the virtual world; the risk of becoming a victim of Internet fraud is therefore accordingly high. Based on the suspicious transaction reports filed with the A-FIU, cases of fraudulent sale of goods and services which are not delivered, or misappropriation of assets using fraudulently obtained account details to withdraw the victim's funds, are particularly common.

Although the fraud tactics described often rely on the gullibility of the victims, there is also an increase in practices that can deceive even experienced people. These include, in particular, investment fraud and CEO fraud. Perpetrators induce companies to make payments to certain accounts by pretending to be a senior member of staff and by building up time pressure. Employees can be duped by the appearance of authority and authorise transactions as instructed.

Most common predicate offences to money laundering: Blackmail

A new trend towards the predicate offence of blackmail/extortion (Art. 144 *et seq.* StGB) has also recently become apparent in connection with cybercrime and money laundering. Often perpetrators use encryption programs to encrypt the victims' personal data or their whole operating system (ransomware attack), or cause servers to be unavailable by carrying

out distributed denial of service (DDoS) attacks. During these attacks, the perpetrators extort money from the victims by promising to decrypt the data or to call off the DDoS attack.

Most common predicate offences to money laundering: Drug-related crime

Offences against the Narcotic Substances Act [*Suchtmittelgesetz*, German acronym: SMG] also frequently occur in connection with money laundering investigations, so the risk of these offenses being committed is to be assessed as high. The police crime statistics for the last three years show an annual average of 22 cases of money laundering. Illicit handling of narcotic substances pursuant to Art. 27 SMG and preparation of trafficking in narcotic substances pursuant to Art. 28 SMG were also investigated in connection with those cases.

The offence frequency and the associated high risk can be attributed, *inter alia*, to the widespread distribution and relatively high availability of narcotic substances. However, the number of suspicious transaction reports received by the A-FIU does not reflect the offence frequency; the reasons for this are that preparation of trafficking in narcotic substances (Art. 28 SMG) is merely a preparatory offence, and that lower amounts of payments are often made in cases of illicit handling of narcotic substances (Art. 27 SMG). Payments are usually processed without using the services of professional groups subject to reporting obligations. Drug-related transactions often take place via the informal transaction system Hawala.

Most common predicate offences to money laundering: Organised crime

Any person who knowingly acquires, holds, invests, administers, etc. proceeds that are subject to the control of a criminal organisation or a terrorist organisation (Art. 165 para. 3 StGB) is deemed to commit a special form of money laundering; a specific predicate offence is not required. The police crime statistics for the last three years show an annual average of four cases of investigations for money laundering in which it was suspected that asset components of a criminal group or organisation were being laundered. Although these numbers are low in absolute terms, the risk must be assumed to be high due to the high criminal energy of such groups and the dangers posed by them.

The fact that none of the suspicious transaction reports received by the A-FIU is based on the assumption of the presence of a criminal organisation is probably due to the fact that, unlike a specific predicate offence, it is even more difficult to identify the connection between the transaction and a specific type or level of organisation.

Most common predicate offences to money laundering: Human trafficking and people smuggling

Criminal organisations also regularly fund their activities by means of human trafficking and people smuggling. Forced prostitution and migrant smuggling are lucrative sources of income for criminal organisations.

Victims of human trafficking often come from vulnerable populations and are exposed to high levels of coercion; they are often afraid to make a report at all. In the case of (successful) people smuggling, there are no victims in the strict sense of the word, and the individuals being smuggled rarely make a (voluntary) report. The number of unreported cases in this offence area is accordingly high. Nevertheless, the risk can be assumed to be high due to the considerable damage to society and to the victims.

The analysis of some of the suspicious transaction reports received by the A-FIU, however, shows a different picture and thus indirectly confirms the assumption that there is a high number of unreported cases in this offence category. The category of “Other” in Figure 1

also contains suspicious transaction reports that were filed due to the fear that the transactions reported in the STR might not have been made voluntarily, but under duress. Although analyses of these suspicious transaction reports often cannot provide any proof of coercion, they usually suggest that the transactions are carried out by prostitutes. Due to the high transaction values and the frequency of such transfers, it cannot be ruled out that these persons are transferring funds for a third party.

Most commonly detected methods of money laundering

Cryptocurrencies

Despite significant price fluctuations, cryptocurrencies are still a tried and true means of money laundering. Incriminated money can be exchanged for cryptocurrencies relatively easily via trading platforms. For a fee, transactions can be disguised with the help of so-called mixers or tumblers, so that the origin of the funds can no longer be proven. This poses a particular challenge for law enforcement authorities in general, and thus also for the A-FIU. Cryptocurrency can now also be loaded onto prepaid cards so that it can be directly available in the real economy.

Money mules

Developments in the area of financial agents remain a cause for concern.
Financial agents are individuals who are often recruited by criminal organisations to transfer assets generated by illicit means. Contact with potential financial agents is made mainly via the Internet, through job offers promising lucrative earnings for little effort.
The task of the individuals who are recruited in this way is to receive transfers to their account and forward them as instructed. The target accounts are dispersed worldwide. By means of international transfers and by involving multiple identities, the funds are concealed as the perpetrators intended.

Hawala

Hawala is an informal worldwide transaction system. Its oriental roots date back to the early Middle Ages. It is based on trust, which is created through common linguistic, ethnic and religious identifiers. This system still endures in the age of the Internet and online banking systems. In general, it is often used by people with a migrant background and by the families they leave behind, especially in developing areas and crisis zones. It is often used for so-called “remittances” (transfers back to their countries of origin). In this way, funds can be transferred quickly and anonymously, even to remote areas without the appropriate infrastructure and connectivity to international payment systems. It leaves no digital traces.
The potential for use of the Hawala system is especially high in industry sectors that conduct cash-intensive transactions in their daily business operations and regularly maintain foreign business relationships involving an accordingly large number of associated foreign transactions.
Recent findings indicate that in Austria the Hawala system is used in particular in the field of drug trafficking and people smuggling.

Forgery of documents

Although forgery of documents is expressly mentioned in Art. 165 StGB as a predicate offence to money laundering, in practice it is rarely the assets obtained through forgery of documents that give rise to suspicion of money laundering. Rather, forgery of documents usually serves as a means of committing money laundering. For example, perpetrators present fake identity documents when opening accounts. Stolen passports or identity cards, with the perpetrator’s photograph affixed, are often used for this purpose.

The use of forged registration forms has recently become particularly common. By using a forged registration form, perpetrators feign a domestic place of residence, which is required to open an account in Austria.

Combating fraud, tax, customs and money laundering

Fraud and smuggling in the customs sector

General information

In practice, predicate offences to money laundering fall under three main groups: Under-invoicing, over-invoicing and smuggling.

Over-invoicing is payment in excess of the true value of the goods in order to generate money for corruption or embezzlement and consequently black money.

Under-invoicing of imported goods in the customs sector occurs, in particular, in connection with Customs Procedure Code 42xx. In these cases, customs duties are collected in the Member State which carries out the customs clearance. After customs clearance, an intra-Community delivery of goods is made to the destination country, where the import value-added tax (VAT) should be paid.

Smuggling occurs, in particular, in the area of excise duties on cigarettes, petroleum products, counterfeit medicines and drugs.

Threat

Threats are presented by three offences.

Over-invoicing
Generating funds in connection with a predicate offence, e.g. corruption or embezzlement, which are then placed in circulation in the context of money laundering.

Under-invoicing
Threats are present in the case of fraud involving the code 42xx procedure. For honest traders, this customs procedure has the advantage that import VAT is not collected at the time of customs clearance. On the other hand, this procedure poses high risks for the customs and tax administrations in the Member States (MS) of the European Union. For example, under-invoiced invoices which sometimes show only 10% of the actual goods value are presented for customs clearance in the importing country. A number of checks have also revealed excess quantities when compared to the information in the shipping documents. This leads to massive reductions in customs duties in Austria and throughout Europe. Furthermore, in many cases import VAT is not paid in the destination country, the invoice recipients often do not exist (so-called “missing traders”) and some of the goods are diverted to other countries. Some end up in European black markets or enter legal trade once they have been made cheaper by the aforementioned fraudulent practice. Diversion scenarios via other Member States have also been reported.

Smuggling
This is a particularly lucrative predicate offence due to the high excise duty charges. In 2019, in 2,062 cases a total of 4,989,552 cigarettes and 5.9 tonnes of other smoking tobacco was seized.

Conclusion:
In summary, the threat should be classified as moderately significant.

Vulnerability

(a) Risk exposure:
High volumes of goods movements across third-country borders, as well as the involvement of numerous public and private parties, make transparency and tracking difficult.

(b) Risk awareness:
There is a high level of risk awareness in the public and private sectors.

(c) Legal framework and supervision/governance:
All three scenarios described above are criminalised by the Financial Crimes Act. In the area of smuggling, random checks are carried out.
The customs authority has a risk assessment in place, on which its IT systems are based; those systems assign a separate risk level to each category of goods and determine the frequency of checks by customs officers.

Human and financial resources:
A total of 271.6 full time equivalents are available, divided between the specialised anti-fraud unit, training and customs offices.

Conclusion:
In summary, the vulnerability is classified as moderately significant.

Risk-mitigating measures

The Customs Administration carries out ongoing identification of fraud scenarios and the perpetrators involved. In addition, preventive action is taken by providing guidelines and training for employees. Together with the Member States, the EU Commission has developed pan-European indicators and criteria for identifying under-invoicing, which are applied by the MS. A profile has been created for customs clearance and subsequent checks at the recipient freight forwarder's premises.

Overall risk

There is a moderately significant risk associated with the three scenarios.

Recommendations

If one Member State puts successful measures in place, the perpetrators immediately take refuge in the next Member State. The problem can only be solved on an EU-wide basis.

Predicate tax offences

General information

Fiscal offences as predicate offences to money laundering (Art. 165 StGB):

- Tax evasion pursuant to Art. 33 Financial Penal Act [German acronym: FinStrG] for amounts above EUR 100,000
- Smuggling under Art. 35 FinStrG for amounts above EUR 50,000
- Evasion of import or export duties under Art. 35 FinStrG for amounts above EUR 50,000
- Intentional handling of goods on which tax or duty has been evaded under Art. 37 FinStrG for amounts above EUR 50,000
- Cross-border VAT fraud under Art. 40 FinStrG

Threat

Below is a non-exhaustive list of threat scenarios for the predicate offences referenced above. Over the last decade, the courts have handed down an average of around 150 convictions per year.

Threat scenarios

- The customer or client receives monies, and the documents (invoice) come from an offshore sanctioned country
- The customer or client is a welfare recipient or has only a low official income, but receives regular transfers from other accounts, possibly with an invoice number.
- The customer or client regularly transfers monies to or receives monies from known cryptocurrency exchanges. Documents (invoice) come from an offshore sanctioned country
- The customer or client is listed as a sham trader in the list of sham traders
- A large proportion of transactions are settled in cash

These scenarios often occur in combination. The greatest threats are generally related to scenarios with an offshore connection.
It can be seen from the conviction figures that predicate offences under financial criminal law pose a constant risk.

Conclusion:
In summary, the threat should be classified as moderately significant.

Vulnerability

(a) Risk exosure:
There is no need to assess risk exposure, as this is an analysis of predicate offences.

(b) Risk awareness:
There is very good risk awareness in the area of tax administration.
In the financial sector, risk awareness is basically good, whereas it varies in the non-financial sector.

(c) Legal framework and supervision/governance:
The legal framework is comprehensively regulated by tax legislation.

Human and financial resources:
A total of 8 full-time equivalents (FTEs) are available, divided between the anti-fraud specialist department, the risk management unit (PACC) and the Anti-Fraud Office, which are responsible for processing STRs related to money laundering.
It should also be noted that all staff at the Tax Authority Austria and the audit unit for large traders notify the competent units wherever there are indications of predicate offences.

Conclusion:
In summary, the vulnerability is classified as moderately significant.

Risk-mitigating measures

Training courses are given in the public and private sectors. The risk management department (PACC) regularly conducts risk assessments in connection with predicate offences.

Overall risk

In summary, the risk should be classified as moderately significant.

Recommendations

Ongoing training and further education measures, and implementation of risk assessments.

Fraud with offshore links

General information

The term "offshore" includes both classic tax havens and jurisdictions that systematically permit low taxation (15% or lower direct tax) or tax concessions (either as a general principle or for a limited period of time). They also allow the client a high degree of anonymity.

Offshore constructs serve the following purposes:

- No taxes or low taxes in the destinations concerned, combined with a high degree of confidentiality due to strict banking secrecy as well as concealment of the identity of the beneficial owner and the transactions, and the impossibility of exchanging information due to a lack of mutual assistance / mutual legal assistance treaties.
- Where treaties have been concluded, no content-related information is transferred, as economic activity in the territory in question is prohibited.

Threat

Offshore constructs are a significant indicator of money laundering. Offshore leaks (e.g. PANAMA papers, LUX leaks, etc.) have revealed a large number of crimes facilitated by offshore jurisdictions. Offshore structures are used not only for tax evasion, but also to commit a number of criminal offences such as fraud, fraudulent bankruptcy and embezzlement, as well as malfeasance by public servants (corruption/bribery).

The following threat scenarios were observed in Austria:

Case study 1:
An offshore company opens a domestic account and uses it to receive incoming foreign payments from companies that are actually operating entities and from offshore companies. The accumulated account balances are withdrawn in cash or forwarded. There are hardly any ways to investigate these cases domestically, since the underlying transaction does not

take place in Austria. Furthermore, it is virtually impossible to determine the identity of the actual beneficial owner of the company. Foreign nationals are authorised to represent the company. It seems reasonable to assume that this type of construct is being used for money laundering.

Case study 2:
An offshore company has a domestic business address and/or a domestic bank account. Administrative tasks – "mailings", "accounting", "telephone redirection", "payment instructions", etc. - are carried out from the domestic business address. Criminal investigations in Austria are rarely possible, since the underlying business is not conducted in Austria and the identity of the actual beneficial owner is not known. There are huge account transactions, the information - if any is available - is not meaningful and does not enable criminal investigations to be initiated. It seems reasonable to assume that this type of construct is being used for money laundering.

Case study 3:
An Austrian legal entity is a subsidiary of a foreign offshore company. It was founded by a foreign trustee and may be administered from Austria as well as from the foreign country. If goods are delivered, they are invoiced only via Austria – with no VAT - but the payments often refer to "intellectual services" such as "feasibility studies", "consultancy agreements", etc. There are huge account transactions. Austrian nationals act as managing directors, members of the board or shareholders. The legal entities have identical company addresses. They issue sham invoices for fictitious underlying business transactions. It seems reasonable to assume that this type of construct is being used for money laundering.

<u>Conclusion</u>:
In summary, the threat should be classified as very significant.

Vulnerability

(a) Risk exposure:
The legal system and the public authorities permit foreign clients to pay low rates of tax and simultaneously assure them of a high degree of confidentiality through banking secrecy and privacy rules. Furthermore, information concerning transactions cannot be exchanged due to a lack of mutual assistance/ mutual legal assistance treaties.
In 2019 the Austrian Tax Administration made 211 requests to offshore destinations. There is rarely any response.

(b) Risk awareness:
Both public authorities and the private sector are highly aware of the risks associated with structures with links to offshore jurisdictions.

(c) Legal framework and supervision/governance:
The following legislation is intended to reduce anonymity in economic transactions with a foreign connection and to promote the exchange of information:
Automatic exchange of financial account information pursuant to Art. 91 Common Reporting Standard Act [German acronym: GMSG] (DAC 2-CRS), the EU Mandatory Disclosure Act [German acronym: EU-MPfG], the Double Taxation Convention (German acronym: AHE), Commission Delegated Regulation (EU) 2016/1675 pursuant to Art. 9 para. 2 of Directive (EU) 2015/849, as amended.

Human and financial resources:
One full-time equivalent is provided for in the Anti-Fraud Department.
In the course of the Tax Administration's activities, the Anti-Fraud Office regularly makes requests to offshore destinations.

Conclusion:
In summary, vulnerability should be classified as very significant.

Risk-mitigating measures

In addition to the legal framework referenced above, the following risk-mitigating measures are in place:

- Training of obliged entities, regular cooperation between competent authorities and obliged entities, BEPS (Base Erosion and Profit Shifting) measures.
- Reinforcement of the duty of cooperation in foreign cases in the area of fiscal procedures (see Art. 115 para. 1 Austrian Federal Fiscal Code [German acronym: BAO]), treatment in the FMA circular on due diligence obligations.
- The Accounts Register provides the authorities with important information concerning the prevention and combating of money laundering and terrorist financing.

Overall risk

In summary, the risk should be classified as very significant.

Recommendations

International exchange of information should be facilitated and reinforced by means of international agreements.

Virtual currencies and cryptoassets

General information

Virtual currencies are defined by Art. 2 no. 21 Financial Markets Anti-Money Laundering Act [German acronym: FM-GwG].

Threat

In the SNRA summary scenarios, the risk of abuse of virtual currencies for money laundering was classified as significant. In the text that follows, we will analyse the national risk.

Due to the current limited regulation and supervision in the crypto sector, criminals are increasingly turning to these payment methods. Predicate offences are also being committed in connection with cryptoassets due to the rapid increase in their popularity. This includes, in particular, the spread of ransomware demanding ransom payments in cryptocurrency. In the dark web, cryptocurrencies are the only payment option.
Cryptocurrencies are used for concealment in the area of money laundering.

Conclusion:
Based on the SNRA summary scenarios, which suggest a significant threat, the current national data show that there is a very significant threat.

Vulnerability
In the SNRA summary scenarios, the vulnerability of virtual currencies to abuse for purposes of money laundering was classified as significant/very significant. **(a) Risk exposure:** Since anonymity makes it more difficult to access information about financial streams and user data, these are also more difficult to investigate. This varies depending on the type and technical design of the cryptocurrency. It is difficult for authorities to secure the access code to a wallet containing potential illicit asset components. Investigations by law enforcement agencies as well as seizure of assets and executions are made more difficult as a result. Traceability of financial flows is also significantly weaker compared to the regulated fiat financial sector. **(b) Risk awareness:** Both the public sector and the private sector show a high level of risk awareness. **(c) Legal framework and supervision/governance:** Due to an amendment to the FM-GwG, providers of virtual currencies are now also obliged entities. They are therefore subject to the due diligence obligations of the FM-GwG, and they must register with and are supervised by the FMA. **Conclusion:** Based on the SNRA summary scenarios, which suggest significant/ very significant vulnerability, the general conditions we have presented here mean that the **vulnerability of virtual currencies to exploitation for purposes of money laundering should be classified as significant.**
Risk-mitigating measures
The Federal Ministry of Finance participates in research projects with other authorities, the private sector and the academic sector. The research projects also feed into staff training. One full-time equivalent (FTE) is allocated within the Anti-Fraud Department. The funding for the research projects amounts to 1.6 million euros over four years.
Overall risk
The overall risk should be classified as very significant.
Recommendations
International exchange of banking information for tax purposes should be extended to the crypto sector. The continuing research projects should enable the authorities to gain a comprehensive understanding of the sector.

ANNEX. The Accounts Register as a measure to combat fraud and money laundering
General information
The Accounts Register provides the authorities with important information for preventing and combating money laundering and terrorist financing. Data quality is improved by means of automated procedures and controls. Public prosecutors' offices, criminal courts, federal

tax authorities, financial criminal authorities, the Federal Tax Court, the FIU, BVT, BK, BAK, FMA and OeNB are authorised to query the Register.
Recommendations
There are gaps due to the lack of loan accounts and the limited scope of application as regards providers who do not offer safe deposit box services as their main activity. Recording of account balances would result in an improvement of the available information.

Terrorist financing threat scenarios

Risk of terrorist financing
General information
Any person who provides or collects **assets** with the intention that they will be used, even if only in part, to commit ... terrorist offences ... (Art. 278d StGB). **Assets** are tangible, intangible, movable or immovable items of property, regardless of how acquired, legally relevant documents or deeds (electronic/digital) evidencing rights to or in assets, bank loans, travellers' cheques, bank cheques, money orders, shares, securities, bonds, bills of exchange, letters of credit, etc.
Threat
At present, the financing of terrorism is primarily limited to the maintenance of terrorist groups. The management of this type of group, even if it is not located in a crisis zone, requires financial resources for strategic tasks such as propaganda and recruiting new members, and for covering the organisational costs or living expenses of its key personnel. Compared to the 1970s and 1980s, when Austria was still a target country for terrorist attacks, it has since become a transit country and a country of refuge, where financing, recruitment and propaganda activities are carried out. In 2020, 707,780 (in 2015: 566,000) third-country nationals were living in Austria. Around 42% of them come from the Western Balkans. Approximately 16% are Turkish citizens. Today, 96,425 people (or 13.6%) come from the so-called "Arab Spring" countries. 47,766 people (or 6.7%) come from the Afghanistan/Pakistan crisis zone. 32,872 people (or 4.6%) have Russian citizenship. A large proportion of these people come from the North Caucasus. All these areas are, or have been until recently, conflict zones (Turkey, the North Caucasus, the former Yugoslavia, Afghanistan, Iraq, Syria). In addition, for about 15 years there has been a trend towards jihadi travel by Austrian converts or third-country nationals living here, first to Afghanistan and since 2013 to Syria and Iraq, which is a more recent phenomenon, as these converts did not belong to terrorist groups in Austria, but joined the various groups in the crisis zones. A considerable number of people have left or tried to leave for Syria and Iraq. Since the destruction of ISIS, this trend has been in sharp decline, and family members and friends of these jihadi travellers are keen to help their friends or relatives return home, or to obtain their release from captivity. The potential danger posed by returnees from jihad cannot be determined, because while some have been rehabilitated in the interim, others still cling to their radical ideas. **Fundraising - Donations:** Terrorist organisations collect funds mainly within their own communities and use very clandestine methods. The more the donors identify with the organisation's "cause", the easier it is to raise funds. Sympathisers of terrorist organisations often have only very limited financial resources. Nevertheless, it is well known that fundraising can sometimes generate considerable amounts of money. Funds are collected through intermediaries or via unregulated crowdfunding forms. In 2012, a two-person association used an unregulated crowdfunding form to raise the sum of € 22,000 in a short space of time, the official aim of the collection being for a humanitarian purpose abroad. The true purpose is (usually) unknown

to the many small donors. Furthermore, making a donation is a commandment in many religions and usually consists of small and very small amounts. Well-organised groups operate (cultural) associations, promoting the cultural purpose of the association to the outside world as a cover for the true purpose of the group.

Transfers to third countries:
Funds for financing terrorism are almost exclusively destined for third countries (the Russian Federation, Turkey, the Middle East, Somalia, Afghanistan, Pakistan, Iraq, Syria, etc.), making it practically impossible to reliably determine the final destination and ultimate recipient, as funds are sometimes also transferred via other third countries.

There is also evidence of transfers of funds from family members or close associates of individuals who have travelled to crisis zones and who wish to join or have already joined the armed jihad, as well as those who are still on their way to those zones.

Because of its geographical location, Turkey is a third country which is still frequently used by terrorist groups and their sympathisers for financial transactions when jihadi travellers need to be supplied with funds.
Terrorist organisations targeting Turkey are also active there, meaning that Turkey should also be regarded as a destination country for transactions.
Funds are transferred to the destination country either by official financial service providers (MVTS) or, if this is not convenient or not possible, e.g. if there is no bank account, by unofficial ones (hawaladars). Any number of intermediaries/straw men may be involved for the purpose of disguising the final destination. Terrorist organisations generally use cash couriers for transferring large sums of money, so as to avoid the strict requirements relating to money laundering and terrorist financing to which obliged entities are subject.
Transfers may also be 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 hubs are used by many people for all kinds of motives (to support family in their home countries, trade, etc.).

Therefore, these transfers cannot be placed under general suspicion, since, aside from the argument of lack of infrastructure in the crisis zone, intermediaries are used mainly for personal reasons. Apart from legal financial service providers such as banks and remittance service providers (Western Union, MoneyGram, Coinstar, etc.), transactions are often entrusted to reliable contact persons in the country of origin or the in the recipient country, although as a general rule this is not legally permitted due to the trusteeship they assume. Such trusted individuals are usually compatriots, or at least persons from the same cultural sphere.
Cash couriers may be caught by customs only when entering and leaving EU territory, but on Austrian federal territory this is now only possible at airports and at the borders with Switzerland and Liechtenstein (Art. 17b of the Act on Implementation of Customs Law [*Zollrechts-Durchführungsgesetz*, German acronym: ZollR-DG]).

Suspicious transaction reports:
As can be seen from the row labelled “Cases with the Public Prosecutor’s Office”, only a few suspicious transaction reports submitted to the A-FIU by Austrian financial service providers due to suspicion of terrorist financing lead to actual criminal prosecution, and fewer still result in convictions.

Year	2015	2016	2017	2018	2019	2020
Suspicious transaction reports	113	148	203	167	93	113
Cases with the Public Prosecutor's Office	46	50	54	19	20	3
Convictions	0	0	1	3	2	4

Note 1: Only suspicious transaction reports relating to terrorist financing were counted. However, reports from/ to certain specific destinations are also examined.

Note 2 to 2015: Actually *one* conviction, as one person was convicted under Art. 278b for large-scale collection of funds as part of a terrorist organisation.

In most cases, the (main) reasons given by the financial service providers submitting STRs are suspicious customer behaviour and the fact that the name or parts of the name of the client or recipient match the names of persons or organisations on sanctions lists (EU, UN, OFAC, etc.). Reporting entities also refer to conspicuous values and frequencies of transactions.

The quality of STRs has been steadily improving. This is probably due to the routine that has become established among reporting entities. However, this is still subject to variability.

It is important that obliged entities, in addition to checking objective criteria such as similarities of names, sanctions lists or specific destinations, always weigh all of the circumstances (know your customer). Individuals and organisations using the services of a financial service provider for the purpose of terrorist financing are aware that their actions are subject to monitoring, hence there must be a general assumption that individuals will (attempt to) conceal the actual use of the funds, for example by giving a false reason for a donation.

However, actual observation of customer behaviour is becoming increasingly difficult in view of the changing banking policy, which is moving away from the counter and towards “online business”. Indeed, there are already questions about the effectiveness of the Austrian “know your customer” system (keyword: online registration).

As soon as a financial service provider switches to de-risking and blocks a customer's account, and that person can, in the end, no longer find a bank willing to open an account or make transfers, the person disappears altogether from the view of the obliged entities, and indirectly from that of the supervisory and police authorities, as they either arrange transactions via the informal money transfer network (Hawala) or through straw men, or switch to alternative means of payment such as Bitcoin.
Finally, it should be noted that, for the purpose of determining whether the transfer in question had a terrorist purpose, it is almost impossible to determine the end purpose of money transfers abroad.

Relevant threats in Austria:
In Austria, legal sources of financing or disbursement of funds for terrorist organisations and individuals are used, e.g. through donations (collections), earned income, social welfare, and also loans, etc. No instances of raising money through criminal acts (robbery, theft, fraud, etc.) have been detected to date. Funds for small groups or individuals who participated or attempted to participate in jihad in Syria/ Iraq were usually raised from their own resources and by family and friends.

Risks of proliferation financing

Risk of proliferation

General information

The Federal Agency for the Protection of the Constitution and Counterterrorism (German acronym: BVT) and the 9 Provincial Agencies for the Protection of the Constitution and Counterterrorism are the authorities responsible for police investigations into proliferation activities or sanctions violations.

In the area of export controls, weapons, military goods and dual-use goods are subject to permits. The BVT is involved in the decision-making processes in the area of export controls, and as such makes an important contribution to preventing illegal transfers of goods.

In addition, the BVT also coordinates interministerial cooperation in national efforts to combat proliferation. Current national and international developments are discussed in meetings across authorities, and joint measures and their effects are debated.

Threat

Combating proliferation will continue to be one of Austria's central security tasks. The danger of weapons of mass destruction, carrier systems, dual-use goods and corresponding expertise falling into the hands of sanctioned regimes or terrorist organisations, or of certain goods being exploited for purposes of proliferation contrary to official statements, represents one of the major risks relating to proliferation.

In this context, Austria is not only a transit country for goods connected to proliferation, but also a target for illegal procurement activities due to its highly developed industrial manufacturing sector and the large number of small and medium-sized enterprises that are world leaders in some areas. Dual-use goods, i.e. materials or products that, due to their sophistication, can be used in both the civilian and military sectors, pose a particular problem.

Closely related to the phenomenon of proliferation is that of money laundering. The number of reports from the banking sector shows that the awareness and sensitivity of Austrian financial service providers to the challenges referenced above have increased significantly.

This heightened sensitivity is also true for the implementation of international sanctions in connection with non-proliferation.

Analytical reports relating to money laundering all indicate an increase in both the complexity and the creativity of concealment methods. This fact demonstrates the need to continue raising awareness of the dangers of illicit financing and funds in order to counter the risks.

Considering the large number of international or intra-state conflicts and the misuse of weapons of all kinds by sub-state groups that could come into possession of chemical, biological, radioactive or nuclear materials, the risk factor for the area of proliferation increases considerably.

Risk-mitigating measures
As part of a national awareness programme, an initiative to raise export-specific awareness in the Austrian economy, the BVT also informs a large number of companies of current problems in order to investigate and prevent the involvement of domestic companies in illegal procurement practices at an early stage.

Risks of legal entities and trusts

Legal entities and trusts can be abused for the purposes of money laundering and terrorist financing. Therefore, their specific risks have been analysed. The Registry Authority has carried out a detail analysis to this end, which also forms the basis for the risk-based supervision of the Beneficial Ownership Register.

Legal entities and trusts

General information

The scope of application of the Beneficial Owners Register Act (BORA [German acronym: WiEReG]) includes a total of 366,719 legal entities as of 1 January 2021. The following legal entities are recorded in the Register of Beneficial Owners, broken down by legal form:

	Number		Number		Number
Partnerships (OG, KG)	65,634	**Insurance associations and savings banks**	80	**Associations**	126,187
Public limited companies	976	**European legal forms (EEIG, SE and SCE)**	43	**Charitable foundations and funds**	629
Limited liability companies	168,398	**Private foundations**	3.033	**Trusts**	4
Commercial and industrial cooperative societies	1,700	**Other legal entities**	33	**Arrangements similar to trusts**	2

Transparency of beneficial owners:
The legal forms listed above are legal entities pursuant to Art. 1 para. 2 BORA and must therefore report their beneficial owners to the Register of Beneficial Owners. The Register of Beneficial Owners also contains information on whether the shares in a legal entity are held by a beneficial owner on its own behalf or acting as a trustee for a trustor. The reporting rate of legal entities subject to the reporting obligation is 96.09%, and that of all legal entities is 89.83%. Automatic data import is performed for 67.86% of the legal entities.

Maintaining the Register of Beneficial Owners:
The Register of Beneficial Owners is maintained by the Registry Authority established at the Federal Ministry of Finance. The tasks of the Register Authority include functional and technical management, conducting administrative proceedings, analysing and checking reports, filing breaches of reporting obligations and responding to enquiries by telephone and in writing. A total of six employees (FTE) are currently employed to handle these tasks. The Tax Authority Austria (Finanzamt Österreich) hands out fines to enforce the reporting obligations. The Anti-Fraud Office (Amt für Betrugsbekämpfung) sanctions the violation of reporting obligations.

Threat

Money Laundering & terrorist financing:
In the SNRA summary scenarios, the threat of abuse of legal entities or legal arrangements for terrorist activities was classified as moderately significant. The threat related to money laundering, conversely, was classified as significant. In the text which follows, we will analyse the threat for each respective legal form. The calculations are done separately, with the results for money laundering (ML) and terrorist financing (TF) presented together; any differences are shown separately at the appropriate points.

Geographic threat:
In order to determine the geographic threat, an analysis was performed of the proportions of beneficial owners with a place of residence in Austria, in other Member States, in third countries and in third countries with a risk of terrorist financing or money laundering, in comparison to the total number in the Register. The risk class in each case is based on the relevant value for high-risk third countries (<0.5% lowly significant; <1% moderately significant; <1.5% significant; >1.5% very significant):

Legal form	Domicile of beneficial owner					Citizenship of beneficial owner					TF threat	ML threat
	Domestic	MS	Third country	High-risk third country (TF)	High-risk third country (ML)	Domestic	MS	Third country	High-risk third country (TF))	High-risk third country (ML)		
Partnerships (OG, KG)*	96.6%	2.7%	0.6%	0.01%	0.01%	82.5%	8.9%	8.6%	1.13%	0.70%	**significant**	**moderately significant**
Public limited companies	79.7%	11.0%	9.3%	0.00%	0.06%	74.3%	17.7%	7.9%	0.00%	0.00%	**lowly significant**	**lowly significant**

Limited liability companies	90.3%	6.4%	3.3%	0.02%	0.03%	85.3%	10.0%	4.7%	0.11%	0.18%	**lowly significant**	**lowly significant**
Commercial and industrial cooperative societies	99.5%	0.4%	0.1%	0.00%	0.00%	99.2%	0.7%	0.1%	0.00%	0.00%	**lowly significant**	**lowly significant**
Insurance associations and savings banks	100%	0.0%	0.0%	0.00%	0.00%	98.9%	1.1%	0.0%	0.00%	0.00%	**lowly significant**	**lowly significant**
European legal forms (EEIG, SE and SCE)	42.9%	46.0%	11.1%	0.00%	0.00%	51.1%	44.4%	4.4%	0.00%	0.00%	**lowly significant**	**lowly significant**
Private foundations	90.9%	4.8%	4.3%	0.01%	0.03%	91.0%	6.0%	2.9%	0.03%	0.01%	**lowly significant**	**lowly significant**
Other legal entities	98.1%	1.9%	0.0%	0.00%	0.00%	84.6%	9.6%	5.8%	0.00%	0.00%	**lowly significant**	**lowly significant**
Associations	99.2%	0.7%	0.1%	0.00%	0.00%	95.8%	2.8%	1.4%	0.22%	0.13%	**lowly significant**	**lowly significant**
Charitable foundations and funds	97.0%	2.1%	0.8%	0.00%	0.00%	93.0%	5.3%	1.7%	0.04%	0.00%	**lowly significant**	**lowly significant**

Trusts	52.9%	47.1%	0.0%	0.00%	0.00%	23.5%	76.5%	0.0%	0.00%	0.00%	**lowly significant**	**lowly significant**
Arrangements similar to trusts**	0.0%	0.0%	0.0%	0.00%	0.00%	0.0%	0.0%	0.0%	0.00%	0.00%	**significant**	**significant**
AVERAGE	**86.1%**	**11.2%**	**2.7%**	**0.00%**	**0.01%**	**79.9%**	**16.6%**	**3.4%**	**0.14%**	**0.09%**		

* For **partnerships,** the geographic threat is classified as **significant (TF)** or **moderately significant (ML)**. The citizenship profile of beneficial owners is significantly more international than average, and the proportion of third countries with a risk of terrorist financing is over 1% across those citizenships.

**** For **arrangements similar to trusts**, no meaningful data were available at the time the risk assessment was prepared. The indicators for those were therefore assessed as "**significant risk**".

Economic threat:

To determine the economic threat, an analysis was performed as to which proportion of each legal form carries out its main activity in a high-risk economic sector (<5% lowly significant; <10% moderately significant; <15% significant; >15% very significant). Any differences between money laundering and terrorist financing are taken into account by incorporating the results of the Supranational Risk Assessment:

Legal form	**Main activity in high-risk economic sectors**		**Threat**
	Absolute	Relative	
Partnerships (OG, KG)	14,452	22.02%	**very significant**
Public limited companies	411	42.11%	**very significant**
Limited liability companies	50920	30.24%	**very significant**
Commercial and industrial cooperative societies	444	26.12%	**very significant**
Insurance associations and savings banks	22	27.50%	**very significant**
European legal forms (EEIG, SE and SCE)	43	39.53%	**very significant**
Private foundations	2953	97.36%	**very significant**
Other legal entities	3	9.09%	**moderately significant**
Associations	239	1.68%	**lowly significant**
Charitable foundations and funds	3	0.48%	**lowly significant**
Trusts*	N/A	N/A	**very significant**
Arrangements similar to trusts**	N/A	N/A	**very significant**
AVERAGE (mean value)		**29.61%**	

* There are no data available on the proportion of **trusts** with their main activities in high-risk economic sectors, due to lack of ÖNACE records. However, due to the purpose of asset management generally pursued by trusts, they are comparable to private foundations in terms of economic risk, hence the **very high** risk class, which is consistent with the analysis data for private foundations.

** There are no meaningful data available for **arrangements similar to trusts** either, as no ÖNACE codes were assigned for the two arrangements similar to trusts which are registered in Austria. The same assumption applies to those as to trusts.

Susceptibility of specific legal forms:

In the SNRA, the main criteria used to determine the threat were the complexity of formation, the knowledge required, and the legal and economic operating costs. Any differences between money laundering and terrorist financing are taken into account (if they are not addressed separately) by incorporating the results of the SNRA. Based on those assumptions, the following statements can be made for the respective legal forms:

Legal form	Susceptibility of specific legal form	Reason
Partnerships (OG, KG)	**lowly significant**	A very prominent feature of registered partnerships is the direct involvement of the partners, who all appear in the publicly accessible Commercial Register. These legal forms are also less attractive for purposes of abuse due to the unlimited personal liability of all partners of a general partnership (OG) and all general partners of a limited partnership (KG), and the difficulty in transferring company shares (extent of participation not visible in the commercial register, consent of all other partners required). These statements apply only in part to limited partnerships ("GmbH und Co KG"); however, numerous provisions of stock company law apply to these companies (e.g. duty to prepare annual accounts).
Public limited companies	**lowly significant**	A notary must be involved in all important measures adopted by the company, and overall transparency is very high due to a number of registration obligations in the publicly accessible commercial register. The legal requirements for the company and the mandatory involvement of credit institutions also ensure that the shareholders (legal owners) can always be reliably determined. In addition, the legal and economic costs of operation are high.
Limited liability companies	**TF: lowly significant** **ML: moderately significant**	A notary or a credit institution must be involved in many important measures adopted by the company, and overall transparency is very high due to a number of registration obligations in the publicly accessible commercial register. Since the shareholders are registered on the publicly accessible commercial register, the legal owners of the company can be determined. However, shares in limited liability companies can be transferred relatively easily and quickly, despite the need to involve a notary, making this particular legal form more susceptible to money laundering (e.g. through the possible sale of "shell companies").
Commercial and industrial cooperative societies	**lowly significant**	This is a very specific legal form and is therefore not "inconspicuous" from the outset in business dealings. It is subject to regular audits due to the legal requirement of membership of an audit association and periodic audits of the financial statements by an auditor appointed by the audit association. The fact that commercial and industrial cooperative societies generally have a large number of members may also make this legal form very unattractive fo purposes of money laundering.
Insurance associations and savings banks	**lowly significant**	Formation of these legal entities is subject to extensive requirements, as well as a very high degree of transparency due to mandatory registration on the commercial register and comprehensive reporting and information obligations *vis-à-vis* the FMA. In addition, the legal and economic costs associated with their operation are high due to extensive governance requirements.

European legal forms (EEIG, SE and SCE)	**lowly significant**	For EEIGs, reference should be made to the risk class for partnerships (especially OGs), for SEs to that of public limited companies, and for European Cooperative Societies (SCEs) to the risk class for commercial and industrial cooperative societies. The requirement of a cross-border element for all three European legal forms means that the costs incurred in forming or operating them tend to be even higher than for the respective national legal forms.
Private foundations	**moderately significant**	As a general principle, a notary must be involved in many important measures adopted by the foundation, and overall transparency is high due to a number of registration obligations in the publicly accessible commercial register. Transparency is also ensured by the requirement to report the beneficial owners, including beneficiaries, classes of beneficiaries, one-time and ultimate beneficiaries, as well as all persons otherwise exercising control. Registration on the commercial register is a formation requirement, which also ensures that all private foundations are recorded on the Commercial Register and the Register of Beneficial Owners. In addition, the foundation's management board must immediately notify the tax office responsible for collecting corporate income tax electronically of the identities of the beneficiaries.
Other legal entities	**lowly significant**	The legal and financial requirements for formation are generally very extensive. The details of the strict governance requirements are regulated by the respective underlying laws. Since other legal entities must by definition be registered on the commercial register, and since they are individually created entities whose sponsors are usually regional authorities, transparency is very high.
Associations	**TF: significant** **ML: moderately significant**	In contrast to other legal forms (e.g. limited liability companies), the identities of the active persons are not verified and the legal costs associated with formation and operation are also low. The applicable governance requirements vary according to the size of an association and provide for an external audit by an auditor if the amount of ordinary income and expenditure is above three million euros. On the other hand, it must be borne in mind that an association may only be founded for non-material purposes and not with the aim of making a profit. However, associations can play an important part in collecting donations, which in turn could be used for purposes of terrorist financing. The susceptibility of this specific legal form to terrorist financing should therefore be classified as increased. Associations with an annual income from donations collected from the public of more than one million euros in two consecutive annual accounting periods must prepare extended annual financial statements (balance sheet, profit and loss account, notes) pursuant to Art. 22 para. 2 of the Associations Act [German acronym: VerG], and must also have their financial statements audited by an auditor.
Charitable foundations and funds	**lowly significant**	The identities of the active persons are not verified, and as long as certain size limits are not exceeded, the costs associated with formation and operation are moderate. In terms of risk mitigation, however, it should be taken into account that for ordinary income and expenditure of above one million euros in two consecutive years, an external audit by a foundation or fund auditor must be ensured and a balance sheet, profit and loss account and management report must be prepared. This means that operational costs are significantly increased and external controls are reinforced. It must also be borne in mind that the foundation or fund assets pursuant to Art. 1 of the Federal Act on Foundations and Funds [German acronym: BStFG] and the income from these may be used only for charitable or benevolent activities.
Trusts	**very significant**	Setting up a trust does not involve uniform formal requirements or compulsory entries in public registers. There is also no requirement to involve notaries or lawyers. In addition, there is no general obligation under trust law to disclose the existence of a trust if the trustee acts on its behalf. It should also be noted that, in contrast to other legal forms, there is no mandatory verification of the identities of the persons involved and both the legal and economic costs associated with formation and operation are very low. Full coverage in the Register of Beneficial Owners cannot be ensured, since the independent reports of the trusts are the only source of data collection.
Arrangements similar to trusts	**very significant**	Setting up an arrangement similar to a trust does not involve uniform formal requirements or compulsory entries in public registers. There is also no requirement to involve notaries or lawyers as a general principle. It should also be noted that - if no legal professions representing the parties which are involved

		in the formation - there is no requirement to verify the identities of the persons involved and both the legal and economic costs associate with formation and operation can be very low. Full coverage in the Register of Beneficial Owners cannot be ensured, since the independent reports by the arrangements similar to trusts are the only source of data collection.

Recently observed typical threat scenarios:

Abuse of the legal form: A threat scenario observed in connection with **terrorist financing** concerns associations as possible vehicles for transferring funds abroad for purposes of terrorist financing. These are usually associations which 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 aid projects advertised, or only reach them in part. The recipients of payments are often natural persons or foreign associations in countries severely impacted by terrorism, where the use of the funds cannot be verified due to a lack of evidence or records. Abuse of the association by third parties: Domestic charitable associations act as aid organisations in crisis zones and use local helpers whose background can never be fully ascertained (Source: BVT).

In relation to **money laundering,** the use of limited liability companies to disguise the origin of financial resources was identified as a threat scenario. In this case, several companies (or shell companies acquired specifically for this purpose) are used to channel financial streams along the constructed chain of companies. For the companies involved, fictitious managing directors from abroad are used (mostly from Eastern European countries), who are also registered as shareholders on the commercial register, but who have no insight into the business activities of the company. The true beneficial owners are also concealed in this way. The limited liability companies involved are usually active in the construction industry or increasingly also in trade, especially within Europe, and are linked to one another by orders or fictitious invoices. The funds thus forwarded are ultimately withdrawn in cash and sent abroad. One characteristic is that when the managing director withdraws cash, there is often another person present to supervise that fictitious managing director. Many of the intermediary companies have employees, at least for a short time, and typically there is also social contributions fraud and subsequent insolvency of individual companies. The *de facto* directors cannot be reached in person. Limited liability companies are attractive for this threat scenario because the legal form is particularly well suited to fast company takeovers. According to the list of legally established sham companies published by the Federal Ministry of Finance, as of 26 February 2021, more than half of the companies listed are limited liability companies (Sources: Unit I/9, Federal Ministry of Finance; FIU).

Potential concealment of beneficial ownership:

Whether an attempt is actually being made to conceal beneficial owners of legal entities can also be assessed on the basis of the irregularities found in the Register of Beneficial Owners (the highest value is decisive: Remarks/trusteeships (Treuhandschaften): <0.5% lowly significant; <1% moderately

significant; <1.5% significant; >1.5% very significant; Non-transparent foreign legal entities: <1% lowly significant; <3% moderately significant; <4% significant; >5% very significant):

Legal form	Remarks	Reported trustee relationships	Non-transparent foreign ultimate legal entities	Threat assessment
Partnerships (OG, KG)	0.03%	0.43%	1.11%	**moderately significant**
Public limited companies*	0.32%	1.17%	7.08%	**very significant**
Limited liability companies	0.08%	1.49%	2.26%	**significant**
Commercial and industrial cooperative societies	0.00%	0.00%	0.00%	**lowly significant**
Insurance associations and savings banks	0.00%	0.00%	0.00%	**lowly significant**
European legal forms (EEIG, SE and SCE)*	0.00%	2.38%	8.33%	**very significant**
Private foundations	0.63%	1.48%	0.00%	**significant**
Other legal entities	0.00%	0.00%	0.00%	**lowly significant**
Associations	0.00%	0.00%	0.00%	**lowly significant**
Charitable foundations and funds	0.19%	0.40%	0.00%	**lowly significant**
Trusts**	0.00%	0.00%	0.00%	**very significant**
Arrangements similar to trusts**	0.00%	0,00%	0.00%	**very significant**
AVERAGE	**0.10%**	**0.61%**	**1.57%**	

* Due to the potential concealment of beneficial ownership observed, a **very significant threat** emerges for **public limited companies and European legal forms,** where the decisive factor is the share of non-transparent foreign supreme legal entities, which is significantly above 5%.

** With regard to **trusts (or arrangements similar to trusts)**, it should be noted that complete coverage of trusts falling within the scope of the BORA cannot be ensured due to the fact that the independent entry on the supplementary register is the only source of data for other parties concerned. The above figures only allow conclusions to be drawn in regarding disclosure of the beneficial owners of those trusts that were registered on the supplementary register. It is not possible to draw any conclusions as to the number of those trusts whose trustees have not satisfied their obligation to register the trust on the supplementary register. Due to the lack of verifiability, it can therefore be assumed that there is a **very significant** potential for concealment.

Vulnerability

Money Laundering & Terrorist Financing:
In the SNRA summary scenarios, the susceptibility/vulnerability of legal entities or legal arrangements was classified as significant with regard to abuse both for purposes of terrorist financing and of money laundering. In the text which follows, we will analyse the legal form-specific vulnerability. The corresponding results are calculated separately for money laundering and terrorist financing but presented together; any differences are shown separately at the appropriate points.

(a) Risk exposure:
In accordance with the general assessment, the risk exposure should be assumed to be **significant** according to the Supranational Risk Assessment. The following legal form-specific peculiarities exist:
Savings banks & insurance associations: In derogation from the general assessment, the risk exposure here should be classified as **lowly significant.** Due to the ongoing supervision by the FMA in combination with the strict legal requirements for foundation, the appointment of the authorised representatives and the continuous record-keeping, it should be very difficult for potential perpetrators to exploit this legal form for purposes of terrorist financing.
Other legal entities: In derogation from the general assessment, the risk exposure should be assumed to be **lowly significant,** due to the special features of the legal form in relation to its formation and its association with the public sector and the associated restrictions and oversight mechanisms.
Associations: In derogation from the general assessment of the Supranational Risk Assessment, the risk exposure should be assumed to be **moderately significant**, since associations may only be founded for non-material purposes and may not be profit-oriented. Due to the typical areas of application of this legal form, it will also not be possible to process larger transactions via the accounts of an association without these being conspicuous in the transaction monitoring of the credit institutions. However, associations can be used to collect donations to a limited extent. However, if these exceed one million euros in two consecutive years, the associations are required to prepare an extended annual financial statement and to appoint an auditor. It should be noted, however, that the possibilities to verify the actual use of funds are often limited in practice (e.g. because funds are sent abroad and it is not possible to perform local verification of their use at the destination).
Charitable foundations and funds: In derogation from the general assessment of the Supranational Risk Assessment, the risk exposure should be assumed to be **moderately significant,** since charitable foundations and funds may only be formed for the achievement of charitable or benevolent purposes and may not be aimed at profit. Since funds may only be withdrawn in accordance with the purpose, and since according to Art. 2 para. 1 of the Federal Act on Foundations and Funds [German acronym: BStFG] it must be ensured that the remaining assets do not fall below 50,000 euros, this legal form is not suitable for the collection and forwarding of donations.

(b) Risk awareness:
In line with the general assessment, a **moderately significant** level of risk awareness should be assumed. However, there are the following special features specific to legal form:
European legal forms: As these legal forms are very rarely used, a **lowly significant** level of risk awareness should be assumed, in derogation from the general assessment.
Trusts and **arrangements similar to trusts:** In derogation from the general assessment, a **lowly significant** level of risk awareness should be assumed for these legal entities, as the use of these legal structures is not common in Austria and therefore the knowledge of the obliged entities in this regard might not be sufficient.

(c) Legal framework and supervision/governance:
With regard to the legal framework and supervision/governance, we analyse the legal requirements for notaries and lawyers upon formation, governance requirements and reporting compliance for each legal form (reporting compliance is composed in equal part of the reporting rate and the frequency of remarks; reporting rate: >95% very significant; >90% significant; >80% moderately significant; <80% low compliance; frequency of notations: <0.05% very significant; <0.1% significant; <0.5% moderately significant; >0.5% lowly significant compliance):

Legal form	Legal requirements*	Governance requirements*	Reporting quota	Frequency of remarks	Reporting compliance
Partnerships (OG, KG)	**very significant**	**moderately significant**	98.81%	0.03%	**very significant**
Public limited companies	**very significant**	**very significant**	95.79%	0.32%	**significant**
Limited liability companies	**very significant**	**significant**	98.80%	0.08%	**very significant**
Commercial and industrial cooperative societies	**very significant**	**significant**	97.70%	0.00%	**very significant**
Insurance associations and savings banks	**very significant**	**very significant**	95.68%	0.00%	**very significant**
European legal forms (EEIG, SE and SCE)	**very significant**	**significant**	74.50%	0.00%	**significant**
Private foundations	**very significant**	**very significant**	97.88%	0.63%	**significant**
Other legal entities	**very significant**	**very significant**	84.84%	0.00%	**significant**
Associations**	**lowly significant**	**moderately significant**	73.04%	0.00%	**significant**
Charitable foundations and funds	**lowly significant**	**significant**	81.08%	0.19%	**moderately significant**

Trusts	**lowly significant**	**lowly significant**	100.00%	0.00%	**very significant**
Arrangements similar to trusts	**lowly significant**	**lowly significant**	0.00%	0.00%	**lowly significant**
AVERAGE			**89.83%**	**0.05%**	

* More detailed information on the legal requirements or governance requirements can also be found in the comments on legal form-specific susceptibility.

Associations have a relatively low reporting rate of 73.04%, presumably due to the fact that many planned general meetings could not be held in 2020 because of COVID-19 and therefore no new election or extension of the term of office of the representative bodies took place, which are automatically imported to the Register of Beneficial Owners, since an exemption from the obligation to report applies.

Risk-mitigating measures

- Obligation of the legal entities to annually identify and verify the beneficial owners and to report to the Register of Beneficial Owners
- Ensuring mandatory reporting through an automated coercive penalty procedure
- Risk-oriented analysis and review of incoming reports by the Registry Authority and financial penalties of up to 200,000 euros for incorrect reports
- Mandatory inspection of the register for obliged entities upon the establishment of a business relationship combined with the duty to make a remark in the event of incorrect reports
- Multiple options for integrating the Register into the ongoing processes of obliged entities via a web service connection and a change service

Overall risk

The calculation method for overall risk is as follows: **Overall risk** = 40% threat + 60% vulnerability - risk-mitigating measures.
The overall risk is broken down by legal form in the **following table** (lowly significant risk: 1-1.5; moderately significant risk: 1.51-2.5; significant risk: 2.51-3.5; very significant risk: 3.51-4. All values with significant or very significant risk are highlighted in red):

	Threat*		Vulnerability**		Residual risk		Legal form-specific risk	Risk-mitigating measures***	Overall risk	Class
	TF	ML	TF	ML	TF	ML	TF/ML			

Partnerships (OG and KG)	2.3	2.5	2.2	2.1	2.2	2.3	**2.22**	-0.55	**1.66**	**moderately significant**
Public limited company	2.2	2.5	1.9	1.9	2.0	2.2	**2.08**	-0.52	**1.56**	**moderately significant**
Limited liability company	2.1	2.8	2.0	2.0	2.0	2.3	**2.17**	-0.54	**1.63**	**moderately significant**
Commercial and industrial cooperative societies	1.8	2.2	1.9	1.9	1.9	2.0	**1.95**	-0.49	**1.46**	**lowly significant**
Insurance associations and savings banks	1.8	2.2	1.3	1.3	1.5	1.6	**1.55**	-0.39	**1.16**	**lowly significant**
European legal forms (EEIG, SE and SCE)	2.2	2.5	2.4	2.4	2.3	2.5	**2.38**	-0.60	**1.79**	**moderately significant**
Private foundations	2.3	2.6	2.0	2.0	2.1	2.2	**2.17**	-0.54	**1.63**	**moderately significant**
Other legal entities	1.6	1.9	1.4	1.4	1.5	1.6	**1.55**	-0.39	**1.16**	**lowly significant**
Associations	1.9	1.9	2.6	2.6	2.3	2.3	**2.32**	-0.58	**1.74**	**moderately significant**
Charitable foundations and funds	1.3	1.7	2.5	2.5	2.0	2.2	**2.10**	-0.53	**1.58**	**moderately significant**
Trusts	2.8	3.2	3.3	3.3	3.1	3.2	**3.15**	-0.79	**2.36**	**moderately significant**
Arrangements similar to trusts	3.2	3.5	3.8	3.8	3.5	3.7	**3.58**	-	**3.58**	**very significant**

* The **risk** is calculated as follows: Result of Supranational Risk Assessment: 1/3, result of National Risk Assessment: 2/3 (of which geographical risk, economic risk, legal form-specific susceptibility and risk scenarios observed each accounts for 1/4).

** **Susceptibility/vulnerability** is calculated as follows: Risk exposure: 1/4, Risk awareness: 1/4, Legal framework and supervision: 1/2 (of which legal requirements for notaries and lawyers upon formation, governance requirements and reporting compliance each accounts for 1/3).

The effectiveness of the **risk-mitigating measures** is assumed to be 1/4 of the total risk before deduction of the risk-mitigating measures. This does not apply to arrangements similar to trusts, as those had a reporting rate of 0% as of 1 January 2021.

Recommendations

The Register Authority should implement the following measures:

- Further improvement in data quality should be achieved, on the one hand, by further development of the risk-oriented supervision based on the results of the National Risk Assessment (internal measures) and, on the other, by improving the reaction of the obliged entities to detected inaccuracies in the Register of Beneficial Owners (external measures)
- The legal form-specific reporting rates should be subject to ongoing monitoring and legal form-specific measures should be taken

- The integration of the Register of Beneficial Owners into individual and standardised software products should be further prioritised in order to facilitate digital processes and simplify the practical handling of the Register
- With regard to the risk scenarios observed, risk-mitigating measures should be developed in cooperation with the authorities concerned
- Cooperation with the tax authorities and the Anti-Fraud Office (Amt für Betrugsbekämpfung) should be intensified in order to further increase reporting compliance
- Cooperation with supervisory authorities of obliged entities, the Financial Intelligence Unit and the BVT should be intensified and knowledge transfer should take place in the form of workshops

The supervisory authorities should pay particular attention to the following points when checking compliance with due diligence obligations by obliged entities:

- Implementation of the obligation to take insight into the Register of Beneficial Owners when establishing a new business relationship and to update the data on beneficial owners
- Implementation of the duty to report remarks in cases of incorrect beneficial owner data to the Register

Sector risk assessment – Financial sector

Financial sector/Funds with credit and financial institutions (CIs/FIs)
General information
In many cases, CIs/FIs are the first points of contact for introducing funds into the mainstream financial system. Their wide distribution and accessibility, as well as their relatively low costs, also make CI/FI services attractive for purposes of ML/TF. The Austrian financial sector has traditionally been characterised by a large number of CIs. Apart from their strong market penetration in the domestic financial centre, Austrian FIs are also very strongly represented in foreign markets (especially in the CESEE region), as evidenced in particular by the number of (foreign) subsidiaries and branches.
Threat
Terrorist financing: In the SNRA summary scenarios, the threat of assets at CIs/FIs being abused for terrorist activities was classified as significant to very significant. There are risks because terrorists and their supporters use the classic financial system to raise funds (through both legal and illegal activities) to support terrorist activities, but also to transfer (small) amounts of money to areas where terrorist acts are to be carried out. **Conclusion:** **In summary, the threat should be classified as significant.**
Money laundering: In the SNRA summary scenarios, the threat was classified as very significant. Due to the large number of financial products and services offered by CIs/FIs, as well as handling payment services, there is a particular risk that they might be abused for money laundering purposes. Transactions in connection with cash, prepaid cards and cash-equivalent financial assets with high liquidity (e.g. time deposits or deposits), in particular, carry an increased risk. Other types of accounts, such as certain forms of fiduciary accounts (see the Regulation on Due Diligence for Fiduciary Accounts [German acronym: AndKo-SoV]) or school savings accounts (see the School Savings Schemes Due Diligence Regulation [German acronym: Schulspar-SoV]) may be associated with a lower risk. **Conclusion:** **In summary, the threat should be classified as significant.**
Vulnerability
Terrorist financing: In the SNRA summary scenarios, the vulnerability of assets at CIs/FIs in relation to exploitation for purposes of terrorist financing was classified as significant. In the text which follows, we will analyse the national vulnerability.

(a) Risk exposure:
The FMA collects data on all transactions to and from every country in the world (those data refer to each individual country and include all incoming and outgoing transactions). Of the total number of transactions on the Austrian financial market, only a small number are directed to high-risk countries or crisis zones (or adjoining countries) or originate from such countries.

(b) Risk awareness:
The FMA data also show that only a small number of CIs/FIs carry out such transactions.

(c) Legal framework and supervision/governance:
Pursuant to Art. 9a FM-GwG, business relationships and transactions involving high-risk third countries result in such customers being classified as high-risk and enhanced due diligence obligations must be applied in addition to the due diligence obligations that must be applied in any case. Furthermore, the factors that increase the risk set out in Annex III to Art. 9 FM-GwG must also be borne in mind when assessing the risk of a client.

Conclusion:
Based on the SNRA summary scenarios, which suggest significant vulnerability, the framework conditions we have presented here lead us to class the vulnerability of assets at CIs/FIs to exploitation for purposes of terrorist financing as moderately significant.

Money laundering:
In the SNRA summary scenarios, the vulnerability of assets at CIs/FIs to exploitation for purposes of money laundering was classified as significant. In the text which follows, we will analyse the national vulnerability.

(a) Risk exposure:
The Austrian CI/FI structure is very heterogeneous and serves a variety of different customer and business segments. These range from regionally limited, classic retail and commercial business, through international corporate and investment banking, to international private banking.

(b) Risk awareness:
The Austrian financial market covers a broad customer spectrum. This includes business relationships with off-shore customers, foreign correspondent banks, business relationships with politically exposed persons (PEPs), foundations, non-profit organisations (NPOs) or other customer relationships which, based on their typologies, may have an increased risk (such as business relationships with customers from regions with an increased geographic risk). As an international banking centre, Austria is traditionally also attractive to foreign customers.

(c) Legal framework and supervision/governance:
See under TF, above.

Conclusion:
Based on the SNRA summary scenarios, which suggest significant vulnerability, the framework conditions we have presented here lead us to classify the vulnerability of assets at CIs/FIs to abuse for purposes of money laundering as significant.

Risk-mitigating measures
Due to the size of the CI/FI sector in Austria and its importance to the Austrian financial market, as well as the ML/TF risk described, this sector is the focus of supervision by the FMA. This is also reflected, in particular, in the number of supervisory measures in this sector. The type and intensity of these measures is based, *inter alia*, on the specific risk profiles of the CIs/FIs. This ensures a risk-based distinction between all CIs/FIs in the application of supervisory measures. The A-FIU and FMA present and discuss new developments and methods emerging in the area of ML/TF with the CIs/FIs at joint events, and there is also an in-depth exchange of information by means of a new public-private partnership project.
Overall risk
In summary, the overall risk for both TF and ML should be classified as significant.
Recommendations
Further intensified cooperation between authorities and stakeholders, both to point out current patterns and trends and to take account of findings and observations in the context of further developing the relevant legal frameworks.

Financial sector/Investment companies (KAG) - Real estate investment companies (Immo-KAG) - Alternative investment fund managers (AIFM)
General information
KAGs under the Investment Fund Act [German acronym: InvFG] 2011 and Immo-KAGs under the Real Estate Investment Fund Act [German acromym: ImmoInvFG] formally qualify as CIs in Austria, as the management of investment funds and real estate funds under the InvFG/ImmoInvFG is standardised as a banking activity under the Austrian Banking Act [German acronym: BWG]. However, KAGs and Immo-KAGs have a certain special status in that they are only authorised to provide services in connection with the management of investment funds or individual portfolios under the Securities Supervison Act [German acronym: WAG] 2018. In addition, the Alternative Investment Funds Manager Act [German acronym: AIFMG] provides for licensing or registration for managers of alternative investment funds (AIFs). Both KAGs/Immo-KAGs and (licensed and registered) AIFMs are obliged entities under the FM-GwG and must fully comply with the due diligence and reporting obligations for preventing ML/TF. Clients of KAGs/Immo-KAGs require a custodian, which must be a licensed CI. In particular, the origin of the funds to be invested is thus already verified or complied with by the custodian CI as a first step.
Threat
Terrorist financing: In the SNRA summary scenarios, the risk of KAGs, Immo-KAGs and AIFMs being abused for terrorist activities was classified as lowly significant. From current information and available data, there are no concrete indications of a risk situation in Austria in this respect either. **Conclusion:** **In summary, the threat should be be classified as lowly significant.**

Money laundering:
In the SNRA summary scenarios, the risk was classified as significant.

In the case of investments in investment funds, real estate funds and alternative investment funds, a risk of abuse for money laundering purposes may arise, especially in connection with well-trained individuals (or groups of people) who intentionally exploit such investments and the transactions required in the process to conceal the original source of funds.

Conclusion:
In summary, the threat should be classified as moderately significant.

Vulnerability

Terrorist financing:
In the SNRA summary scenarios, the vulnerability of KAGs, Immo-KAGs and AIFMs to exploitation for purposes of terrorist financing was classified as low. In the text which follows, we will analyse the national vulnerability.
The FMA supervisory practice and the available data and information show that services and products in the KAG/Immo-KAG and AIFM sector do not currently give rise to any particular vulnerability of the Austrian financial market to abuse for purposes of terrorist financing.

Conclusion:
Based on the SNRA summary scenarios, which suggest lowly significant vulnerability, the framework conditions we have presented here lead us to class the vulnerability of KAGs, Immo-KAGs and AIFMs to abuse for terrorist financing as lowly significant.

Money laundering:
In the SNRA summary scenarios, the vulnerability of KAGs, Immo-KAGs and AIFMs to exploitation for purposes of money laundering was classified as moderately significant to significant. In the text which follows, we will analyse the national vulnerability.

(a) Risk exposure:
The FMA supervisory practice and the data and information collected show that services and products in the KAG/Immo-KAG and AIFM sector do not give rise to any particular vulnerability of the Austrian financial market to exploitation for purposes of money laundering, beyond the risk situation described above.

(b) Risk awareness:
As can be seen from the FMA data, the market in Austria in the KAG/Immo-KAG and AIFM sector is relatively small.

(c) Legal framework and supervision/governance:
KAGs/Immo-KAGs and (licenced and registered) AIFMs are obliged entities under the FM-GwG and are subject to FMA supervision in this respect. A client's KYC profile plays an essential role in the provision of services by KAGs/Immo-KAGs and AIFMs. Although unusual transactions or activities may also be consistent with certain typologies in this sector, it is important, especially in the case of services provided by KAGs/Immo-KAGs and AIFMs, that obliged entities have sufficient knowledge of their clients and their investment profiles. In addition to the investment pattern of the customer, the subsequent disposal (e.g. disbursement) of the invested assets must also be taken into account.

Conclusion:
Based on the SNRA summary scenarios, which suggest moderately significant to significant vulnerability, the framework conditions we have presented here lead us to class the vulnerability of KAGs, Immo-KAGs and AIFMs to exploitation for purposes of money laundering as moderately significant.

Risk-mitigating measures

KAGs/Immo-KAGs and AIFMs are covered by the FMA's supervisory measures as obliged entities under the FM-GwG. In this context, the FMA employs on-site measures for preventing ML/TF, both directly at the obliged entities in question, and at the custodian banks and the depository banks. The FMA thus focuses on investments in investment funds, real estate funds and alternative investment funds at the custodian banks and the depository banks.

Overall risk

In summary, the risk for TF should be classified as lowly significant and the risk for ML as moderately significant.

Recommendations

Further intensified cooperation between authorities and stakeholders, both to point out current patterns and trends and to take account of findings and observations in the context of further developing the relevant legal frameworks.

Financial sector/Investment firms (IFs) and investment services providers (ISPs)

General information

In addition to CIs, IFs/ISPs authorised to provide investment services on a commercial basis under the WAG 2018 are also relevant to the provision of investment services. Many investment service providers use external intermediaries acting as brokers (intermediaries or security operators bound by contract) for the investment service provider in their provision of investment services and in sales.

Threat

Terrorist financing:
In the SNRA summary scenarios, the threat of ISPs or IFs being exploited for terrorist activities was classified as lowly significant.

From current information and available data, there are no concrete indications of a risk situation in Austria in this respect either.

Conclusion:
In summary, the risk should be classified as lowly significant.

Money laundering:
In the SNRA summary scenarios, the threat was classified as significant.

Already in the case of investment services pursuant to the WAG 2018, there are many codes of conduct - independent of the provisions in the FM-GwG – which must be complied with from the outset, which will already yield a comprehensive client profile. However, since

clients such as private foundations, clients from third countries, etc. are also being serviced, there is a corresponding residual risk here.

Conclusion:
In summary, the risk should be classified as moderately significant.

Vulnerability

Terrorist financing:
In the SNRA summary scenarios, the vulnerability of ISPs or IFs to abuse for purposes of terrorist financing was classified as low. In the text which follows, we will analyse the national vulnerability.

The FMA's supervisory practice and the available data and information show that services and products in the investment services sector do not currently give rise to any particular vulnerability of the Austrian financial market to exploitation for purposes of terrorist financing.

Conclusion:
Based on the SNRA summary scenarios, which suggest lowly significant vulnerability, the framework conditions we have presented here lead us to class the vulnerability of ISPs or IFs to abuse for purposes of terrorist financing as lowly significant.

Money laundering:
In the SNRA summary scenarios, the vulnerability of ISPs/IFs to abuse for money laundering purposes was classified as significant. In the text which follows, we will analyse the national vulnerability.

(a) Risk exposure:
Both the investor profile and the KYC profile of a client play an essential role in providing investment services. Unusual transactions or activities may also be consistent with certain typologies in this specific field.

(b) Risk awareness:
Due to the varying (personal) circumstances of investors, it is important that investment service providers have sufficient knowledge of their clients, their financial circumstances and their investment profile in order to have the best chance of recognising any deviations from their expected pattern or transactions which have no recognisable economic benefit. In addition to the investment pattern of the client, the focus will in any case be on the subsequent disposal (e.g. disbursement) of the invested assets. In this context, investments with a short investment horizon and a lack of sensitivity to costs incurred are susceptible to increased risk.

(c) Legal framework and supervision/governance:
A wealth of information about the client is obtained through the requirements of the WAG 2018. Independently of this, ISPs/IFs must also comply with the provisions of the FM-GwG and accordingly conduct a risk-based monitoring. Only when this comprehensive analysis has been carried out does the actual transaction take place; here again, the investor's custodian and/or account-holding bank is obliged to carry out another final check. ISPs/IFs are prohibited by law from holding client funds. Thus, each time an account is opened or a transaction is made, it is cross-checked by the investor's custodian and/or account-holding bank.

Conclusion:
Based on the SNRA summary scenarios, which suggest significant vulnerability, the framework conditions we have presented here lead us to classify the vulnerability of ISPs or IFs to abuse for purposes of money laundering as moderately significant.

Risk-mitigating measures

Due to the size of the securities services sector in Austria and its importance to the Austrian financial market as well as the described ML/TF risk, this sector is the focus of FMA supervision. This is also reflected, in particular, by corresponding on-site audits in this sector. Commercial investment advisors (Art. 136a of the Trade Act [German acronym: GewO]) and investment intermediaries (Art. 136b GewO) are subject to an ongoing legal obligation to undergo further training which must include the topic of money laundering prevention.

Overall risk

In summary, the risk for TF should be classified as lowly significant and the risk for ML as moderately significant.

Recommendations

Further intensified cooperation between authorities and stakeholders, both to point out current patterns and trends and to take account of findings and observations in the context of further developing the relevant legal frameworks.

Financial Sector/Private banking asset management

General information

The field known as *private banking* is primarily concerned with high-end private clients who invest assets (with a threshold value of EUR 700,000 and above). Often such services also include offerings of complex products, the execution of high-volume transactions and a high level of discretion/confidentiality with regard to the business relationship.

Threat

Terrorist financing:
From current information and available data, there are no concrete indications of a threat situation.

Conclusion:
In summary, the threat should be classified as lowly significant.

Money laundering:
In the SNRA summary scenarios, the threat was classified as significant to very significant.

Private banking client segments can be demarcated by the following specific characteristics: large transaction and/or investment volumes; use of complex products and services; use of legal entities with complex, opaque ownership and control structures (possibly with links to offshore areas - in many cases for tax optimisation reasons), and the client's expectation of increased confidentiality and secrecy. *Private banking* services and products are also exposed to an increased risk of being exploited for purposes of money laundering against the background of the risk factors pertaining to “client” and “geographical areas”. The target group is wealthy private clients with a relatively high proportion of politically exposed persons, including foreign nationals, compared to the classic retail business. Complete

tracing of the origin of the funds used and the actual beneficial owners of these legal entities is made even more difficult by the use of complex corporate structures divided over several cascades, often with links to offshore areas.

Conclusion:
In summary, the threat should be classified as significant.

Vulnerability

Terrorist financing:
The FMA's supervisory practice and the available data and information show that services and products in the field of *private banking* do not currently give rise to any particular vulnerability of the Austrian financial market to exploitation for purposes of terrorist financing.

Conclusion:
Based on the SNRA summary scenarios, which do not suggest any vulnerability, the framework conditions we have presented here lead us to classify the vulnerability of *private banking* services and products to exploitation for purposes of terrorist financing as lowly significant.

Money laundering:
In the SNRA summary scenarios, the vulnerability of services and products in the area of *private banking* to exploitation for purposes of money laundering was classified as significant to very significant. In the text which follows, we will analyse the national vulnerability.

(a) Risk exposure:
The *private banking* sector represents a relatively small proportion of the Austrian financial market as a whole. Based on the data collected by the FMA, it can be deduced that *private banking* clients are concentrated across only a few obliged entities.

(b) Risk awareness:
In terms of the *private banking* sub-risk, 19% of obliged entities are in the low risk class, 69% in the moderately significant risk class and 2% in the significant risk class.

(c) Legal framework and supervision/governance:
Private asset management and *private banking* constitute indicators of potentitally higher risk pursuant to Annex III to Art. 9 FM-GwG. Obliged entities offering services and products in the area of *private banking* must take this into account in both their company and client risk assessments and must implement risk-mitigating measures accordingly. These include, for example, additional information and in-depth documents on the beneficial owner of the client, the origins of the funds used and the purpose and nature of the business relationship (this may be particularly relevant, for example, when dealing with customers from offshore areas who have no further links to Austria and/or do not pursue any operational activities). In addition, institutions must ensure more intensive continuous monitoring of the business relationship (and the transactions) with such clients and shorten the intervals for updating the documents/information obtained.

Conclusion:
Based on the SNRA summary scenarios, which suggest significant to very significant vulnerability, the framework conditions we have presented here lead us to classify the

vulnerability of services and products in the *private banking* sector to abuse for purposes of money laundering as moderately significant to significant.

Risk-mitigating measures

A large number of private banking clients in relation to the total client base represents a risk-increasing factor in terms of the risk classification. Classification in a higher risk class results in more intensive monitoring by the FMA and thus also shortens the interval of the FMA's supervisory measures accordingly, down to annual supervisory measures. The FMA has been conducting and continues to conduct special on-site audits with a focus on the *private banking* client segment at the obliged entities concerned. In this context, there is a particular focus on compliance with due diligence obligations to determine the identity of the client's beneficial owners and on obtaining and verifying information about the origin of the funds used.

Overall risk

In summary, the risk for TF should be classified as lowly significant and the risk for ML as moderately significant to significant.

Recommendations

Further intensified cooperation between the authorities and stakeholders, both to point out current patterns and trends and to take account of findings and observations in the context of further developing the relevant legal frameworks.

Financial sector/Crowdfunding

General information

For the supervisory assessment of crowdfunding in its broader sense, it is important to take into account how the form of the funding is structured in detail. Donation- or reward-based crowdfunding is generally only subject to Austrian financial market supervision laws where the platform also undertakes payment processing between the investors and the projects. In this case, a licence under the Payment Services Act [German acronym: ZaDiG] 2018 may be required. In contrast, for operating a crowdinvesting platform, the licence requirement depends first on the type of investment and second on the type of platform activity (e.g. credit intermediary platforms or if the investment is structured as a deposit business [licence under the BWG]; platforms which broker transferable securities or other financial instruments or provide personal investment recommendations [licence under the WAG 2018]). In the case of projects in which the receiving company invests in other companies and is not itself operational, the Alternative Investment Funds Manager Act (AIFMG) may generally apply. As a general principle, if a crowdfunding project or the operation of a crowdinvesting platform is subject to one of the supervisory laws referenced above, the provider/operator is also an obliged entity under the FM-GwG. For crowdinvestments issued under the Alternative Financing Act [German acronym: AltFG], the AltFG contains obligations for platforms. If the operator of the platform is not subject to the provisions of the FM-GwG, the provisions of the Trade Act (GewO) on preventing ML/TF under Art. 365m to 365z are applicable (Art. 5 para. 2 no. 1 AltFG). This applies in particular to crowdinvesting in the form of investments, for which at least a trade authorisation for commercial financial consulting pursuant to Art. 136a GewO is required (Art. 5 para. 1 AltFG). The AltFG also

contains obligations for issuers which do not exclusively use a platform (Art. 4 para. 5 AltFG). For this area, supervision is the responsibility of the trade authorities.

Threat

Terrorist financing:
In the SNRA summary scenarios, which encompass all forms of crowdfunding in its broader sense, i.e. including donation- and reward-based crowdfunding, the threat of certain forms of crowdfunding being abused for terrorist activities was classified as moderately significant.

The unregulated "donation-based" crowdfunding sector, in particular, can be abused relatively easily for purposes of terrorist financing. Terrorists or their supporters can use these crowdfunding options to raise funds for terrorist purposes or to support terrorist activities. Based on the available information and data, such threat situations may also arise in Austria.

Conclusion:
In summary, the threat for the regulated sector should be classified as moderately significant and for the unregulated (donation-based, reward-based) sector as moderately significant to significant.

Money laundering:
In the SNRA summary scenarios, which encompass all forms of crowdfunding in its broader sense, i.e. including donation- and reward-based crowdfunding, the threat was classified as moderately significant. From current information and available data, there are no concrete indications of a threat situation in Austria in which crowdfunding is abused for money laundering purposes.

Conclusion:
In summary, the risk should be classified as moderately significant.

Vulnerability

Terrorist financing:
In the SNRA summary scenarios, which encompass all forms of crowdfunding in its broader sense, i.e. including donation- and reward-based crowdfunding, the vulnerability of certain forms of crowdfunding to exploitation for purposes of terrorist financing was classified as moderately significant. In the text which follows, we will analyse the national vulnerability.

(a) Risk exposure:
In Austria, there is a wide network of supervisory provisions which could be applied in connection with crowdfunding projects or platforms. In these cases, the operator is supervised by the FMA in terms of financial market supervision laws in relation to the prevention of ML/TF. In the case of an application of the AltFG, this is the trade authorities' remit.

(b) Risk awareness:
In most cases which do not fall under any of the supervisory laws referenced above, a supervised financial market intermediary is required for onward transfer of the collected funds. As obliged entities subject to the due diligence requirements for prevention of ML/TF, they must pay very close attention to the origin of the funds, particularly when higher cash amounts are deposited or when many small amounts are received within a short period of time, which quickly lead to a large total amount.

(c) Legal framework and supervision/governance:
Operators of crowdfunding projects or platforms must, if they are obliged entities under the FM-GwG or if the AltFG is applicable, fully apply the respective applicable due diligence and reporting obligations. CIs/FIs, as obliged entities under the FM-GwG, must obtain additional information and evidence concerning the origin of funds, especially in the case of (cash) deposits of larger amounts (this represents a risk-increasing factor in any case). This is an important risk-mitigating measure, especially for those areas in which crowdfunding projects or platforms are not subject to any regulation and in which funds are to be collected in smaller amounts for terrorist purposes.

Conclusion:
Based on the SNRA summary scenarios, which suggest moderately significant vulnerability, the framework conditions we have presented here lead us to class the vulnerability of crowdfunding in its broader sense to abuse for purposes of terrorist financing as moderately significant for the regulated sector and moderately significant to significant for the unregulated sector.

Money laundering:
In the SNRA summary scenarios, which encompass all forms of crowdfunding in its broader sense, i.e. also donation- and reward-based crowdfunding, the vulnerability of crowdfunding to abuse for purposes of money laundering was classified as moderately significant. In the text which follows, we will analyse the national vulnerability.

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

Conclusion:
Based on the SNRA summary scenarios, which suggest moderately significant vulnerability, the framework conditions we have presented here lead us to classify the vulnerability of crowdfunding in its broader sense to abuse for purposes of money laundering as moderately significant.

Risk-mitigating measures

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

Overall risk

In summary, the risk of TF should be classified as moderately significant for the regulated sector and moderately significant to significant for the unregulated sector, and the risk of ML should be classified as moderately significant.

Recommendations

Further intensified cooperation between authorities and stakeholders, both to point out current patterns and trends and to take account of findings and observations in the context of further developing the relevant legal frameworks.

Financial sector/Currency exchange offices

General information

Currency exchange offices can be used, in particular, to change (incriminated) funds into higher denomination banknotes. This process may be a first step in connection with cross-border cash transportation. No major preparations or planning are required to carry out a currency exchange transaction, and such an operation can thus be carried out relatively easily.

Threat

Terrorist financing:
In the SNRA summary scenarios, the risk of currency exchange offices being abused for terrorist activities was classified as significant.

Especially in regions close to borders with third countries and at airports, terrorists and their supporters may use currency exchange offices to transport cash to crisis zones in order to support terrorist groups and activities, after having changed it into larger denomination banknotes. In this context, however, there is only an increased risk if currency exchange offices are located in a region close to the border with crisis zones.

Conclusion:
In summary, the threat should be classified as moderately significant to significant.

Money laundering:
In the SNRA summary scenarios, the threat was classified as significant.
Currency exchange offices can be exploited to change incriminated (foreign) funds into euro amounts, possibly in larger denominations.

Conclusion:
In summary, the threat should be classified as moderately significant to significant.

Vulnerability

Terrorist financing:
In the SNRA summary scenarios, the vulnerability of currency exchange offices to abuse for purposes of terrorist financing was classified as significant. In the text which follows, we will analyse the national vulnerability.

(a) Risk exposure:
Due to Austria's geographical location, there is little incentive to change foreign funds (currencies) into larger euro denominations via currency exchange offices in Austria. The potential transport routes for use for terrorist purposes in crisis zones would be long, so there is little incentive for terrorists or their supporters. However, foreign funds (currencies) can be changed into euro amounts via currency exchange offices, and these amounts can then be used to finance terrorist activities in Austria.

(b) Risk awareness:
The withdrawal of the new version of the €500 banknote on 26 April 2019 will gradually reduce the incentive to transport larger amounts of cash in euros.

(c) Legal framework and supervision/governance:
As obliged entities under the FM-GwG, currency exchange offices must fully apply the due diligence and reporting obligations in this respect.

Conclusion:

Based on the SNRA summary scenarios, which suggest significant vulnerability, the framework conditions we have presented here lead us to class the vulnerability of currency exchange offices to exploitation for purposes of terrorist financing as moderately significant to significant.

Money laundering:

In the SNRA summary scenarios, the vulnerability of currency exchange offices to abuse for purposes of money laundering was classified as significant. In the text which follows, we will analyse the national vulnerability.

(a) Risk exposure:

In order to funnel incriminated funds that have been exchanged for euro amounts into the financial system via a currency exchange office, such funds must be deposited with an obliged entity under the FM-GwG (as already stated above under "*Financial sector/funds with credit and financial institutions"*).

(b) Risk awareness:

See under TF, above.

(c) Legal framework and supervision/governance:

Larger amounts of funds, in particular, represent a risk-increasing factor when making a deposit, and the origin of the funds must be particularly scrutinised in such cases. A risk-mitigating factor is the fact that currency exchange offices in Austria, as CIs, require a licence from the FMA and are thus obliged to comply fully with the due diligence and reporting requirements of the FM-GwG.

Conclusion:

Based on the SNRA summary scenarios, which suggest a significant vulnerability, the framework conditions we have presented lead us to class the vulnerability of currency exchange offices to abuse for purposes of money laundering as moderately significant to significant.

Risk-mitigating measures

As CIs, currency exchange offices are obliged entities under the FM-GwG and are therefore covered by the FMA's supervisory measures. In this context, the FMA also conducts on-site visits directly at currency exchange offices.

Overall risk

In summary, the risk for both TF and ML should be classified as moderately significant.

Recommendations

Further intensifed cooperation between authorities and stakeholders, both to point out current patterns and trends and to take account of findings and observations in the context of further developing the relevant legal frameworks.

Financial sector/Electronic money (e-money)

General information

Only electronic money issuers are authorised to issue electronic money. These include mainly CIs and e-money institutions (licence from the FMA). E-money systems can also exist in the form of regional currencies, customer loyalty and bonus point systems and cards for branch networks or corporate groups. Where these systems are what is known as "limited" networks, the issuer is not required to obtain a licence from the FMA.

Threat

Terrorist financing:
In the SNRA summary scenarios, the threat of e-money being exploited for terrorist activities was classified as significant.
For terrorists or their supporters, e-money products can represent advantages over cash, especially if certain activities are to be carried out online (e.g. booking hotels or reserving rental cars). The fact that, since 1 January 2020, anonymous e-money products can no longer be issued in Austria has the effect of mitigating risk in this area. An additional risk-mitigating factor is the traceability of payments using e-money products.

Conclusion:
In summary, the threat should be classified as moderately significant to significant.

Money laundering:
In the SNRA summary scenarios, the threat was classified as significant.
In most cases, e-money products can only be loaded with certain (sometimes relatively small) amounts, as the issuers of such products set certain amount limits themselves.

Conclusion:
In summary, the threat should be classified as moderately significant.

Vulnerability

Terrorist financing:
In the SNRA summary scenarios, the vulnerability of e-money to exploitation for purposes of terrorist financing was classified as significant. In the text which follows, we will analyse the national vulnerability.

(a) Risk exposure:
Although only a small number of e-money issuers operate in Austria under the freedom of establishment, 226 e-money issuers from other Member States are permitted to offer their products in Austria under the freedom to provide services. The latter are not supervised by the FMA with regard to preventing ML/TF, but by the competent supervisory authority in their respective Member State of origin.

(b) Risk awareness:
Since the end of the calendar year 2019, it has no longer been possible to issue anonymous e-money products in Austria, which has made the use of e-money products less attractive for terrorist financing purposes.

(c) Legal framework and supervision/governance:
As obliged entities pursuant to the FM-GwG, e-money issuers must fully apply the due diligence and reporting obligations in this respect and are supervised by the FMA.

Conclusion:
Based on the SNRA summary scenarios, which suggest significant vulnerability, the framework conditions we have presented here lead us to classify the vulnerability of e-money to exploitation for purposes of terrorist financing as moderately significant.

Money laundering:
In the SNRA summary scenarios, the vulnerability of e-money to exploitation for purposes of money laundering was classified as moderately significant to significant. In the text which follows, we will analyse the national vulnerability.

(a) Risk exposure:
See under TF, above.

(b) Risk awareness:
See under TF, above.

(c) Legal framework and supervision/governance:
See under TF, above.

Conclusion:
Based on the SNRA summary scenarios, which suggest significant vulnerability, the framework conditions we have presented here lead us to classify the vulnerability of e-money to exploitation for purposes of money laundering as moderately significant.

Risk-mitigating measures

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

Overall risk

In summary, the risk for both TF and ML should be classified as moderately significant.

Recommendations

Further intensified cooperation between authorities and stakeholders, both to point out current patterns and trends and to take account of findings and observations in the context of further developing the relevant legal frameworks.

Financial sector/Payment services

General information

Payment service providers and e-money issuers domiciled in another Member State which provide services in Austria using service providers, such as agents within the meaning of Art. 4 no. 35 ZaDiG 2018, are subject to the scope of application of the FM-GwG for those services, pursuant to Art. 23 para. 7 FM-GwG. In order to ensure compliance with the provisions on preventing ML/TF and to facilitate supervision by the FMA, these institutions must designate a central point of contact for the FMA if they meet the requirements of the Commission Delegated Regulation (EU) 2018/1108. Within the scope of services provided by payment service providers, particular emphasis should be placed on the product of cash transfers which are not linked to an account.

Threat
Terrorist financing: In the SNRA summary scenarios, the threat of payment services being exploited for terrorist activities was classified as significant. Terrorists or their supporters can use payment services to transfer funds and to receive/send assets for terrorist activities. New payment methods, in particular, can be used (such as via mobile phones, prepaid cards or online payments). **Conclusion:** **In summary, the threat should be classified as significant.**
Money laundering: In the SNRA summary scenarios, the threat was classified as significant. Payment services can be abused for purposes of money laundering, especially in connection with the use of money couriers. In this context, criminal organisations use money couriers to transfer incriminated funds to other jurisdictions without disclosing the actual identities of the parties acting in the background. **Conclusion:** **In summary, the threat should be classified as significant.**
Vulnerability
Terrorist financing: In the SNRA summary scenarios, the vulnerability of payment services to exploitation for purposes of terrorist financing was classified as significant. In the text which follows, we will analyse the national vulnerability. **(a) Risk exposure:** Payments made through payment service providers are not anonymous, but cross-border transactions with high-risk clients or high-risk third countries can be carried out relatively easily. **(b) Risk awareness:** There is an increased risk that Austrian payment service providers will be abused for terrorist financing purposes. **(c) Legal framework and supervision/governance:** Payment institutions, as obliged entities under the FM-GwG, must fully comply with the due diligence and reporting obligations in this respect. One of the most important due diligence obligations in connection with payment services is the identification of the client and any trustees. An additional essential measure is the provision of appropriate training and of the necessary (technical) infrastructure to agents. **Conclusion:** **Based on the SNRA summary scenarios, which suggest significant vulnerability, the framework conditions we have presented here lead us to classify the vulnerability of payment services to abuse for purposes of terrorist financing as significant.**

Money laundering:
In the SNRA summary scenarios, the vulnerability of payment services to exploitation for purposes of money laundering was classified as significant. In the text which follows, we will analyse the national vulnerability.

(a) Risk exposure:
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 the use of payment services for parties other than the direct client is not always disclosed and cannot always be detected.

(b) Risk awareness:
See under (a), above.

(c) Legal framework and supervision/governance:
See under TF, above.

Conclusion:
Based on the SNRA summary scenarios, which suggest moderately significant vulnerability, the framework conditions we have presented here lead us to class the vulnerability of payment services to exploitation for purposes of money laundering as significant.

Risk-mitigating measures

The FMA sets thematic priorities in connection with its on-site measures. In order to ensure that the strategies and processes for preventing ML/TF are also applied to agents, the FMA employs on-site measures jointly at a payment institution and its agents. The FMA's annual risk assessment includes an assessment of the business model of each payment institution. This ensures that payment institutions with higher risk are subject to more intense supervision.

Overall risk

In summary, the risk for both TF and ML should be classified as significant.

Recommendations

Further intensified cooperation between authorities and stakeholders, both to point out current patterns and trends and to take account of findings and observations in the context of further developing the relevant legal frameworks.

Financial sector/Virtual currencies

General information

The high level of potential anonymity in the use of virtual currencies, in particular, makes them attractive for exploitation for purposes of ML/TF (the term "pseudonymity" is used in connection with certain virtual currencies). Although current regulation of virtual currencies in the field of ML/TF prevention is a risk-mitigating factor, new methods (e.g. using so-called "mixers" or "tumblers") and new types of virtual currencies have emerged which increase anonymity still further (so-called *anonymity enhanced currencies; privacy coins*). Transactions in virtual currencies are generally processed outside the traditional financial

services systems. They cannot, therefore, be tracked via the systems used by and already known to CIs/FIs, but require specific (new) monitoring systems. In addition, transactions in virtual currencies are rarely limited to one jurisdiction. Rather, they can be used to carry out widespread cross-border transactions relatively easily and quickly.

Threat

Terrorist financing:
In the SNRA summary scenarios, the threat of virtual currencies being exploited for terrorist activities was classified as significant.

The high level of potential anonymity when using virtual currencies means that terrorists and their supporters can abuse this sector in order to finance terrorist activities. Analyses show that terrorists and terrorist groups are increasingly calling upon their supporters to use Bitcoin and other virtual currencies.

Conclusion:
In summary, the threat should be classified as significant.

Money laundering:
In the SNRA summary scenarios, the threat was classified as significant.

In the field of money laundering, the high level of anonymity in the use of virtual currencies is also a risk-increasing factor. Especially in the area of the *dark web,* payments with Bitcoin or other virtual currencies – which afford a higher level of anonymity – occur frequently. In addition, criminal groups launder such funds by repeatedly exchanging incriminated funds into and out of virtual currencies.

Conclusion:
In summary, the threat should be classified as significant.

Vulnerability

Terrorist financing:
In the SNRA summary scenarios, the vulnerability of virtual currencies to abuse for purposes of terrorist financing was classified as significant. In the text which follows, we will analyse the national vulnerability.

(a) Risk exposure:
Based on the information and data available to the FMA, it can be assumed that there are large disparities in terms of the strategies, controls and processes of individual service providers and their various business models.

(b) Risk awareness:
Based on the information and data available to the FMA, it can be assumed that the individual service providers and their different business models are subject to wide disparities in terms of their understanding and risk awareness.

(c) Legal framework and supervision/governance:
From 10 January 2020, service providers in the field of virtual currencies, as obliged entities under the FM-GwG, must fully apply the due diligence and reporting obligations of the FM-GwG and the EU Funds Transfer Regulation. These service providers must register with the FMA prior to commencing operations.

Conclusion:
Based on the SNRA summary scenarios, which suggest significant to very significant vulnerability, the framework conditions we have presented here lead us to classify the vulnerability of virtual currencies to exploitation for purposes of terrorist financing as significant.

Money laundering:
In the SNRA summary scenarios, the vulnerability of virtual currencies to to exploitation for purposes of money laundering was classified as significant to very significant. In the text which follows, we will analyse the national vulnerability.

(a) Risk exposure:
See under TF, above.

(b) Risk awareness:
See under TF, above.

(c) Legal framework and supervision/governance:
See under TF, above.

Conclusion:
Based on the SNRA summary scenarios, which suggest significant to very significant vulnerability, the framework conditions we have presented here lead us to classify the vulnerability of virtual currencies to abuse for purposes of money laundering as significant.

Risk-mitigating measures

Since virtual currencies in Austria represent a completely new group of obliged entities for compliance with due diligence and reporting obligations, and because of the ML/TF risk described above, this sector is an area of focus of FMA supervision. In 2020, the FMA already carried out four on-site measures to verify compliance with the provisions of the FM-GwG and the EU Funds Transfer Regulation. These service providers must register with the FMA before beginning to provide virtual currency services (16 service providers were registered in 2020). If, in the course of the registration procedure, the FMA has specific indications based on the information and documents provided by the service provider that the requirements of the FM-GwG cannot be met, or if the FMA has doubts concerning the personal reliability of the managing director(s) and the beneficial owner(s) of the service provider or the natural person wishing to act as a service provider, the FMA must refuse registration.

Overall risk

In summary, the risk for both TF and ML should be classified as significant.

Recommendations

Further intensified cooperation between authorities and stakeholders, both to point out current patterns and trends and to take account of findings and observations in the context of further developing the relevant legal frameworks.

Financial sector/"Back-To-Back" business models (Treuhand loans)

General information

In the context of so-called "back-to-back" business models (also called Treuhand loans), upon the order of a trustee, Austrian CIs/FIs grant cash-backed loans to a borrower. In most cases, the trustor is another CI/FI from a third country. The loans to the borrower (debtor) are granted in the name of the Austrian CI/FI but for the account of the trustor. In many cases, the borrowers (debtor) are companies in offshore areas (who often do no operative business).
In principle, "Back-To-Back" business models involve the following business relationships:

1) Deposit transaction: The trustor makes a cash deposit with an Austrian CI/FI.

2) Hedging transaction (contract relationship): By trust order (Treuhandauftrag), the trustor (Treugeber) instructs the Austrian CI/FI to grant loan funds in its own name but for the account of the trustor to a borrower named by the trustor. The trustor's cash contribution is pledged by the trustor to the Austrian CI/FI as collateral.

3) Lending transaction: The Austrian CI/FI grants the loan to the borrower (debtor) in its own name but for the account of the trustor.

For settlement under this business model, the Austrian CI/FI opens an account for the trustor's cash deposit on the one hand and an account for the borrower on the other, to which the loan is disbursed.

Threat

Terrorist financing:
From the current information and data situation, there are no concrete indications of a threat situation in which "back-to-back" business models are exploited by terrorists or terrorist groups for their activities.

Conclusion:
In summary, the threat should be classified as lowly significant.

Money laundering:
In particular, the use of cash as collateral for loans represents an indicator of potentially higher risk for abuse of "back-to-back" business models for money laundering purposes. Another risk-increasing factor in this context is the fact that the loans are not granted on the basis of business decisions by the lending institution, but on the basis of the trustee's mandate. Through "back-to-back" business models, loans are not granted directly by a (foreign) CI/FI to a (in most cases foreign) borrower, but via an (Austrian) CI/FI. The inclusion of additional intermediaries in the processing of credit transactions can reduce their transparency.

Conclusion:
In summary, the threat should be classified as significant.

Vulnerability

Terrorist financing:
The supervisory practice of the FMA and the available data and information show that there is currently no particular vulnerability of the Austrian financial market to abuse for the purposes of terrorist financing through "back-to-back" business models.

Conclusion:
As a result of the framework conditions we have described here, the vulnerability of "back-to-back" business models to abuse for the purposes of terrorist financing should be classified as lowly significant.

Money laundering:

(a) Risk exposure:
At present (as of the end of 2020), there is only a small proportion of Austrian CIs/FIs that offer "back-to-back" business models. Thus, the number of FIs that had "back-to-back" models in connection with guarantees and loans or deposits serving as collateral in their portfolio decreased from five FIs in 2015 with an average share of 30.6 percent of guarantees and deposits in their total loan and deposit portfolio to two FIs with an average share of 2.5 percent of guarantees and deposits in their total loan and deposit portfolio, not least due to the high intensity of supervisory activity by the FMA.

(b) Risk awareness:
Due to the increased risk of money laundering in the area of "back-to-back" business models, the FMA focused its on-site audit activities on verifying compliance with due diligence requirements for preventing ML/TF.

(c) Legal framework and supervision/governance:
In the case of "back-to-back" business models, FIs must apply enhanced due diligence in any event. Due to the high risk of exploitation for money laundering in this area and the supervisory activities of the FMA, FIs have largely exited such business models and now only offer them in a few cases.

Conclusion:
As a result of the framework conditions we have described here, the vulnerability of "back-to-back" business models to abuse for money laundering purposes should be classified as significant.

Risk-mitigating measures

Due to the high ML/TF risk in the realm of "back-to-back" business models, this area was a focus of supervisory activity by the FMA. This was reflected in particular by thematic focal points during on-site audits of those CIs/FIs that have previously offered or continue to offer such business models.

Overall risk

In summary, the risk for TF should be classified as lowly significant and the risk for ML as significant.

Recommendations

Further intensified cooperation between authorities and stakeholders, both to point out current patterns and trends and to take account of findings and observations in the context of further developing the relevant legal frameworks.

Financial sector/Life insurance

General information

In addition to the classic function of a life insurance policy (hedging of risks), such policies also have a savings or financial investment aspect and are thus, like other financial products, subject to abuse for ML/TF purposes. Compared to other financial services, the life insurance sector represents only a relatively small share of the Austrian financial market. Some large Austrian insurance groups are also active in foreign markets (especially CESEE).

Threat

Terrorist financing:
Based on the SNRA summary scenarios, the threat of life insurance being abused for terrorist activities was classified as moderately significant.

From current information and data, there are no concrete indications of a particular risk situation. Above all, the need for very specific know-how makes the use of life insurance less attractive for terrorist financing.

Conclusion:
In summary, the threat should be classified as lowly significant.

Money laundering:
Based on the SNRA summary scenarios, the threat was classified as moderately significant.

Life insurance policies are vulnerable to targeted exploitation for money laundering purposes. This is primarily due to the fact that they can be terminated prematurely and because they can accordingly be redeemed, with disbursement of amounts paid in. However, life insurance contracts usually provide for very unfavourable surrender values for the policyholder in the case of early termination. Another risk factor in connection with life insurance policies is the possibility of selling existing 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 terminated on unfavourable terms. In general, based on current information and data, it may be said that there are no concrete indications of an increased risk that life insurance policies will be used for money laundering.

Conclusion:
In summary, the threat should be classified as lowly significant.

Vulnerability

In the SNRA summary scenarios, the vulnerability of life insurance to abuse for purposes of terrorist financing was classified as lowly to moderately significant. In the text which follows, we will analyse the national vulnerability.

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 give rise to any particular vulnerability of the Austrian financial market to exploitation for the purposes of terrorist financing.

Conclusion:
Based on the SNRA summary scenarios, which suggest lowly to moderately significant vulnerability, the framework conditions we have presented here lead us to classify the

vulnerability of life insurance policies to exploitation for purposes of terrorist financing as lowly significant.

Money laundering:
Under the SNRA summary scenarios, the vulnerability of life insurance policies to exploitation for purposes of money laundering was classified as lowly to moderately significant. In the text which follows, we will analyse the national vulnerability.

(a) Risk exposure:
In Austria, life insurance policies continue to be popular investment products. Following the generally accepted typologies, single premium policies (especially in relation to high cash premiums) represent an increased ML/TF risk.

(b) Risk awareness:
Since the insurance market in Austria is predominantly characterised by domestic business, the majority of policyholders are natural persons residing in Austria.

(c) Legal framework and supervision/governance:
Pursuant to the FM-GwG, insurance companies offering life insurance must fully comply with the ML/TF 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 SNRA summary scenarios, which suggest lowly to moderately significant vulnerability, the framework conditions we have presented here lead us to class the vulnerability of life insurance policies to exploitation for purposes of money laundering as lowly significant.

Risk-mitigating measures

Due to the relatively small number of insurance undertakings that do life insurance business and are required to apply the related regulations on prevention of ML/TF, as well as the homogeneity of risk factors in this sector which goes hand in hand with the fact that they are limited to the life insurance sector, the current supervisory practice of the FMA, especially with regard to the frequency of on-site measures, ensures comprehensive coverage of the insurance sector.

Overall risk

In summary, the risk for both TF and ML should be classified as lowly significant.

Recommendations

Further intensified cooperation between authorities and stakeholders, both to point out current patterns and trends and to take account of findings and observations in the context of further developing the relevant legal frameworks.

Financial Sector/Safe Letting

General information

When providing (letting) safe deposit boxes (safes), the lessor, who bears special security obligations, typically provides the safe deposit boxes with a double lock for a fee.

Threat

Terrorist financing:
Current information and data give no concrete indications of a threat scenario in which the provision of safe deposit box management services is exploited by terrorists or terrorist groups for their activities.

Conclusion:
In summary, the threat should be classified as lowly significant.

Money laundering:
Based on the SNRA's summary scenarios, the threat was classified as significant.
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 use this method to convert such assets into non-incriminated assets.

Conclusion:
In summary, the threat should be classified as moderately significant.

Vulnerability

Terrorist financing:
Based on the supervisory practice of the FMA and the available data and information, it does not appear that services and products in the area of safe deposit box management services currently give rise to any particular vulnerability of the Austrian financial market to exploitation for purposes of terrorist financing.

Conclusion:
Based on the SNRA's summary scenarios, which do not suggest any vulnerability, the framework conditions we have outlined here lead us to classify the vulnerability of services and products in the area of safe deposit box management services to exploitation for purposes of terrorist financing as lowly significant.

Money laundering:
In the SNRA summary scenarios, the vulnerability of safe deposit box management services to abuse for purposes of money laundering was classified as moderately significant to significant. In the text which follows, we will analyse the national vulnerability.

(a) Risk exposure:
The majority of safe deposit box management services offered in Austria are the classic form of safe deposit box rental by licensed CIs.

(b) Risk awareness:
Safe deposit box management services by other companies represent only a low risk; as obliged entities under the FM-GwG, they are also fully subject to the due diligence and reporting obligations of the FM-GwG.

(c) Legal framework and supervision/governance:
The provision (letting) of safe deposit boxes (safes) as a safe deposit box management service is part of the business activities of FIs as defined in Art. 1 para. 2 Banking Act. 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 SNRA summary scenarios, which suggest moderately significant to significant vulnerability, the framework conditions we have presented here lead us to classify the vulnerability of safe deposit box management services to abuse for purposes of money laundering as moderately significant.

Risk-mitigating measures

The FMA may impose administrative penalties for violations of the due diligence and reporting obligations of 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 their obligation to establish and verify the identity of their clients.

Overall risk

In summary, the risk for TF should be classified as lowly significant and the risk for ML as moderately significant.

Recommendations

Further intensified cooperation between authorities and stakeholders, both to point out current patterns and trends and to take account of findings and observations in the context of further developing the relevant legal frameworks.

Financial sector/Business loans

General information

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

Threat

Terrorist financing:
In the SNRA summary scenarios, the threat of business loans being exploited for terrorist activities was classified as lowly significant.

Based on the the information and data available to the FMA, there are no concrete indications of a threat scenario under which terrorist organisations used business loans to finance terrorism.

Conclusion:
In summary, the threat should be classified as lowly significant.

Money laundering:
In the SNRA summary scenarios, the threat was classified as moderately significant.
From the information and data available to the FMA, there are no concrete indications of a threat scenario under which commercial loans are used for money laundering.

Conclusion:
In summary, the threat should be classified as moderately significant.

Vulnerability

Terrorist financing:
Based on the supervisory practice of the FMA and the available data and information, it does not appear that services and products in the area of business loans currently give rise to any particular vulnerability of the Austrian financial market to exploitation for purposes of terrorist financing.

Conclusion:
Based on the SNRA summary scenarios, which suggest lowly significant vulnerability, the framework conditions we have outlined here lead us to classify the vulnerability of business loans to abuse for purposes of terrorist financing as lowly significant.

Money laundering:
Based on the supervisory practice of the FMA and the available data and information, it does not appear that services and products in the area of business loans currently give rise to any particular vulnerability of the Austrian financial market to abuse for purposes of money laundering.

Conclusion:
Based on the SNRA summary scenarios, which suggest moderately significant vulnerability, the framework conditions we have outlined here lead us to classify the vulnerability of business loans to abuse for purposes of money laundering as lowly significant to moderately significant.

Risk-mitigating measures

Pursuant to Art. 1 para. 1 no. 3 Banking Act, the right to conclude loan agreements is reserved for credit institutions and requires a licence from the FMA. In addition to the other due diligence obligations under the FM-GwG, CIs must also obtain sufficient information from customers regarding the origin of funds, for example in the case of loan repayments or repayments that deviate from the original contract. This information must also be accordingly verified by the FI.

Overall risk

In summary, the risk for both TF and ML should be classified as lowly significant.

Recommendations

Further intensified cooperation between authorities and stakeholders, both to point out current patterns and trends and to take account of findings and observations in the context of further developing the relevant legal frameworks.

Financial sector/Consumer credit or small loans

General information

Terrorists and organised crime groups use short-term consumer credit or small loans with high interest rates but low amounts. This can be done, for example, by overdrawing a credit card limit without the intention of repaying this overdrawn amount. Furthermore, consumer credit or small loans can be used for money laundering by buying expensive goods (e.g. vehicles, jewellery) and paying them back early.

Threat

Terrorist financing:
In the SNRA summary scenarios, the threat of consumer or small loans being exploited for terrorist activities was classified as significant.

Terrorist groups or even (radicalised) individuals can use consumer credit or small loans in particular to finance trips by so-called "foreign terrorist fighters" or for themselves in order to travel to crisis regions.

Conclusion:
In summary, the threat should be classified as moderately significant to significant.

Money laundering:
In the SNRA summary scenarios, the threat was classified as moderately significant.

Compared to other financial products, consumer credit or small loans offer little potential for exploitation for purposes of money laundering - especially for "laundering" larger amounts of money.

Conclusion:
In summary, the threat should be classified as lowly to moderately significant.

Vulnerability

Terrorist financing:
In the SNRA summary scenarios, the vulnerability of consumer credit and small loans to exploitation for purposes of terrorist financing was classified as significant. In the text which follows, we will analyse the national vulnerability.

(a) Risk exposure:
The transaction volumes are usually low and control systems are in place at the CIs. However, this does not significantly reduce the risk of vulnerability of the Austrian financial market.

(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 use remote identification options and this is not adequately taken into account by obliged entities.

(c) Legal framework and supervision/governance:
In addition to the further due diligence obligations of Art. 6 FM-GwG, CIs must also, and in particular, have sufficient KYC information regarding the customer. Furthermore, they must set up and appropriately set their transaction monitoring systems.

Conclusion:
Based on the SNRA summary scenarios, which suggest significant vulnerability, the framework conditions presented here lead us to class the vulnerability of consumer or small loans to exploitation for the purposes of terrorist financing as moderately significant to significant.

Money laundering:
In the SNRA summary scenarios, the vulnerability of consumer or small loans with regard to exploitation for money laundering purposes was classified as moderately significant. In the text which follows, we will analyse the national vulnerability.

(a) Risk exposure:
Due to the generally low amounts and the relatively low share of consumer or small loans, the risk exposure of this area is considered low.

(b) Risk awareness:
See above on TF.

(c) Legal framework and supervision/governance:
In addition to the other due diligence obligations of Art. 6 FM-GwG, CIs must also have sufficient information regarding the origin of the customer's funds, for example in the case of loan repayments. Furthermore, they have to install transaction monitoring systems which are appropriately calibrated.

Conclusion:
Based on the SNRA summary scenarios, which suggest significant vulnerability, the framework conditions we have outlined here lead us to class the vulnerability of consumer credit or small loans to abuse for purposes of money laundering as lowly to moderately significant.

Risk-mitigating measures

Pursuant to Art. 1 para. 1 no. 3 Banking Act, the right to conclude credit agreements is reserved to credit institutions. In its on-site audits, the FMA also audits the correct calibration of the transaction monitoring systems by obliged entities.

Overall risk

In summary, the risk for TF should be classified as moderately significant to significant and the risk for ML as moderately significant.

Recommendations

Further intensified cooperation between authorities and stakeholders, both to point out current patterns and trends and to take account of findings and observations in the context of further developing the relevant legal frameworks.

Financial sector/Mortgage loans

General information

Mortgage loans are used to finance real estate by putting up the property to be purchased as collateral for repayment of the loan. In the area of money laundering, the proceeds of crime can be used for real estate investments, for example by using the proceeds for redemption payments or early redemption. In principle, there is also the possibility that terrorists or their supporters may use high-value medium- to long-term mortgage loans to finance their activities.

Threat

Terrorist financing:
In the SNRA summary scenarios, the threat of mortgage loans being exploited for terrorist activities was classified as lowly significant.
The use of mortgage loans for terrorist purposes is difficult, especially because of the fact that they are tied to a property, and due to the associated entry on the land registry and the long-term commitment, and such loans are rarely accessible to terrorists or their supporters.

Conclusion:
In summary, the threat should be classified as lowly significant.

Money laundering:
In the SNRA summary scenarios, the threat was classified as significant.
Mortgage loans can be used for money laundering in order to funnel higher amounts of incriminated funds into the financial system through the purchase of (multiple) properties. Especially by using forged documents and records, organised crime rings try to disguise the actual beneficial owners and the origin of the funds used to purchase real estate. In terms of risk mitigation, one must consider that in the area of mortgage loans, CIs are always involved on such transactions. In addition, the involvement of notaries and lawyers is required to prepare the contract structures and to enter the mortgage on the land registry.

Conclusion:
In summary, the threat should be classified as moderately significant to significant.

Vulnerability

Terrorist 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 SNRA summary scenarios suggesting lowly significant vulnerability, the framework conditions we have outlined here lead us to classify the vulnerability of mortgage loans to exploitation for the purposes of terrorist financing as lowly significant.

Money laundering:
In the SNRA summary scenarios, the vulnerability of bank accounts at CIs/FIs to exploitation for purposes of money laundering was classified as moderately significant. In the text which follows, we will analyse the national vulnerability.

(a) Risk exposure:
Mortgage loans - especially borrowing by private households - represent an important component of the business models of CIs in Austria.

(b) Risk awareness:
Many smaller mortgage loans are taken out for the purchase of housing for owner-occupation. These are relatively small loan volumes. Large-volume - in part also purely speculative - real estate transactions pose a higher risk.

(c) Legal framework and supervision/governance:
In addition to the other due diligence obligations under Art. 6 FM-GwG, CIs must also have sufficient information regarding the origin of the customer's funds, such as where customers are making loan repayments. Furthermore, they must put appropriately calibrated transaction monitoring systems in place.

Conclusion:
Based on the SNRA summary scenarios, which suggest moderately significant vulnerability, the framework conditions we have presented here lead us to classify the vulnerability of mortgage loans to abuse for purposes of money laundering as moderately significant to significant.

Risk-mitigating measures
Due to their increased risk of exploitation for money laundering purposes, mortgage loans are a thematic area of focus of the FMA's on-site audits. Among other things, the FMA examines in detail how credit institutions verify the origin of funds for mortgage loans and check their plausibility against the KYC information. In addition, adequate calibration of the transaction monitoring systems is checked with regard to the repayment modalities.
Overall risk
In summary, the risk for TF should be classified as lowly significant and the risk for ML as moderately significant.
Recommendations
Further intensified cooperation between authorities and stakeholders, both to point out current patterns and trends and to take account of findings and observations in the context of further developing the relevant legal frameworks.

Human and financial resources
The FMA has 27.25 full-time equivalents at its disposal. The competent authorities pursuant to the Alternative Financing Act [*AltFG*] have 0.1072 full-time equivalents at their disposal.

Risk of violation of sanctions

Risk of violation of sanctions
General information
The responsibility of the Federal Agency for the Protection of the Constitution and Counterterrorism [German acronym: BVT] for monitoring compliance with legal rules under the Sanctions Act 2010 follows from the allocation of responsibilities at the Federal Ministry of the Interior. The existing resolutions as well as sanction measures affect several areas. Last but not least, the Austrian National Bank, which is in charge of monitoring financial transactions in the area of credit and financial institutions, also follows the rough subdivision into terrorism (financing), proliferation, as well as country-specific sanctions. All offences within the meaning of the Sanctions Act 2010 involving assets less than Euro 100,000.00 are managed by the district administrative authorities and provincial police directorates as administrative penalty proceedings. The majority of the STRs with regard to possible sanction violations or infringements received by the Money Laundering and Economic Espionage Division of the BVT Intelligence Unit are transmitted to it by the A-FIU. Almost exclusively, these are suspicious transaction reports from banking institutions relating to money laundering. As a rule, reports in connection with financial transactions relate to individual persons as well as companies (mainly sole proprietorships and GesmbHs). To a much lesser extent, reports are made directly by the Federal Ministry of Finance as well as other organisations such as the Federal Ministry for European and International Affairs [German acronym: BMEIA], and rarely anonymously. The clear majority of suspicious transaction reports to the A-FIU by banks and financial institutions is attributed to the sensitive handling of reporting obligations and the resulting, often severe, penalties under the Financial Markets Anti-Money Laundering Act. In connection with the handling of various matters, regular feedback is given to the A-FIU on the progress, in particular, as soon as findings regarding suspicious facts are forwarded to the competent court. Due to the competence of the A-FIU, which is responsible for contacting all credit and financial institutions, no asset or financial investigations are carried out by the specialist department of the BVT's Intelligence Unit. The often difficult demarcation of the factual scenarios between the areas of proliferation and country-specific sanctions makes a statistical survey of the total number of sanction monitoring cases difficult, so that no such survey is currently available. The unit also does not know the number of cases recorded by the OeNB. The BVT processes the STRs in collaboration with the A-FIU, the Federal Criminal Authority (Bundeskriminalamt) and the OeNB on the basis of the applicable resolutions and legal acts. The corresponding UN and EU sanctions lists serve as a basis for this work. In the event of corresponding suspicions, the BVT collaborates closely with the Federal Ministry of Finance, and also reports to the competent court and, based on the value level of the assets involved,

to the relevant district administrative authority or provincial police directorate. The collaboration with these authorities is described as definitely cooperative.
Threat
Accordingly, it was not possible for the BVT, on its own, to provide a complete statistical analysis that could also be used as a basis for assessing the risk of "sanction violations". However, the numbers of STRs regarding the Sanctions Act filed with the specialist unit have not changed significantly in any particular direction over the past few years and, in the overall context, tend to be in the minority.
Recommendations
Both the legal analysis and the evaluation of the underlying facts in respect of terrorism, proliferation and country-specific sanctions are difficult, especially in operational case processing. One possible solution would be to establish a clear procedure for processing cases. The complexity of the subject-matter, in connection with the potential legal consequences and the resulting external impacts, mean that the BVT must strive for a fruitful exchange of information in addition to seeking the relevant legal expertise.

Risk of circumvention of EU financial sanctions against terrorist financing

EU financial sanctions against terrorist financing/financial sector (credit, financial and payment institutions)
General information
The European Union imposes sanctions against terrorist financing in the form of Regulations. This is done both to implement the resolutions of the United Nations Security Council and to enact restrictive measures that are EU-specific. The measures, which are usually implemented by issuing EU regulations on the basis of Art 215 TFEU, apply directly in each Member State in the same way as national law (Art 288 TFEU) and are addressed directly to the persons and bodies who are responsible for applying the law. Thus, for example, banks are also directly bound by them when doing business. In national law, the Sanctions Act 2010 is the relevant legal basis for compliance with sanctions regulations. Restrictive measures are considered an important instrument of the Common Foreign and Security Policy (CFSP), intended to bring about a change in the policies or actions of those against whom the measures are directed, thereby supporting the objectives of the CFSP. Financial sanctions essentially deal with restrictions on capital movements and payments. The reasons for imposing restrictive measures vary and should therefore be treated in accordance with their purposes. This analysis will be limited to restrictive measures against terrorist financing ("listed" terrorists). The classic application of sanctions involves comprehensive duties to freeze funds and economic resources. This goes hand in hand with a corresponding direct and indirect ban on disbursing funds. It is explicitly prohibited for any person to knowingly take actions that lead to or facilitate circumvention of the restrictive measures. It is essential to ensure that no sanctioned person, organisation or institution is directly or indirectly provided with funds or economic resources, that no transactions prohibited under sanctions law are carried out and that no other services are provided that are covered by measures under sanctions law.
Threat
One particular risk is the circumvention of restrictive measures against terrorist financing. This may involve the setting up of non-transparent structures and the exploitation of legal entities, for example by creating complex corporate structures, by interposing fiduciaries or similar non-transparent structures (off-shore, non-operating entities, etc.), which (wilfully) make it more difficult to determine and verify the identity of the actual beneficial owner or the actual economic substance of a transaction. Difficulties of demarcation may arise in the case of transactions that are being entered into with a person, organisation or institution who is not subject to sanctions but whose relationship with a listed person, organisation or institution is close in some way. In this context, it must be considered and examined whether funds and economic resources are being indirectly provided to sanctioned persons, organisations or institutions, as this is also prohibited. It is problematic, for example, if fiduciary relationships are not disclosed and are not otherwise visible to the outside world, or if (concealed) fiduciary structures are created with the help of interposed off-shore entities.

Conclusion:

Due to the risk situation described above, there is an inherent (moderately significant to significant) risk to the financial sector that it may be abused for the purpose of circumventing sanctions rules.

Vulnerability

a) Risk exposure:

In order to recognise and prevent potential violations of sanctions law standards, it is essential for the actual economic substance of transactions to be ascertained as well as the "beneficial owner" to be clearly identified. The implementation of uniform processes and documentation requirements is necessary to prevent violations or circumvention of the norms of sanctions law.

This risk applies in particular in the case of complex, non-transparent corporate structures in which the ownership and control relationships are difficult to ascertain. In cross-border cases, the exchange of information, different legal systems or interpretations of the law, unfamiliar certificates and documents, etc. can also make it difficult to verify the ownership and control structure and the economic substance of a transaction.

(b) Risk awareness:

It has been shown that, to a large extent, the implementation of sanction measures in the financial sector with regard to assets imputable to the persons, organisations or institutions on the respective sanction lists functions well when the requisite systems and processes are in place. The SNRA also assumes that largely functioning sanctions screening is in place (and focuses, in terms of risks, particularly on unlisted (unknown) persons engaging in terrorist activities).

The financial sector has generally been recognised by the FATF as having a good understanding of the threats and risks in the relevant compliance areas.[1]

(c) Legal framework and supervision/governance:

The legal framework is set out primarily in the relevant EU regulations. Administrative and criminal law provisions are codified in Art. 11 Sanctions Act 2010 [SanktG 2010] *et seq.*

The OeNB is responsible for monitoring compliance with sanctions measures in the realm of credit, financial and payment institutions (Art. 8 para. 1 Sanctions Act 2010). For this purpose, the OeNB exercises its monitoring and information powers pursuant to Art. 8 para. 2 Sanctions Act 2010. The OeNB's oversight and information-gathering authorities are also provided for in Art. 5 Foreign Exchange Act 2004 [DevG 2004].

Human and financial resources:

To perform the tasks assigned to the OeNB by Art. 8 para. 1 Sanctions Act 2010 in the area of credit and financial institutions pursuant to Art. 1 Banking Act [BWG] as well as the payment institutions referred to in Art. 4 no. 4 of the Payment Services Act 2018 [ZaDiG 2018, Federal Law Gazette I no. 17/2018], a pool of staff from two departments is deployed as needed: The Legal Department is responsible for the regulatory side of the sanctions regime, whilst the Banking Audit Department conducts on-site audits of credit, financial and payment institutions. EU financial sanctions against terrorist financing are part of the sanctions regime tasks performed by the OeNB. For the year 2021, a total of 1.1 full-time positions has been budgeted for this area of responsibility.

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

Conclusion:

Due to the situation described, there is an inherent risk (moderately significant) that institutions will fail to identify violations or circumventions of sanctions.

Risk-mitigating measures

Measures by institutions:

As a part of their due diligence obligations, institutions must ensure that no funds or economic resources are provided directly or indirectly to any sanctioned person, organisation or institution and that no other transactions which are banned under sanctions law are carried out. In addition, institutions must also comply with their reporting and authorisation requirements. Institutions have put IT tools in place to monitor sanctions-related measures in credit institutions. By means of these systems, transactions as well as the customer portfolio can be checked for issues relevant under sanctions law; on the basis of such checks, transactions can be halted or accounts blocked. When assessing transactions, the basis of the transaction and the economic substance must be taken into account. Circumstances of the individual case must be considered from a risk perspective. For example, the determination of the beneficial owner and the determination of the actual economic substance of a transaction are relevant in this context. Here, too, a risk-based approach by the respective institution in terms of procedures to apply and actions to take is indispensable in order to ensure compliance with due diligence obligations. In addition to ensuring comprehensive customer due diligence and observing the KYC principle, this includes obtaining additional information on the transactions, the origin of the funds used and the purpose and nature of the business relationship. Furthermore, in the case of high-risk customers, institutions must ensure more intensive, continuous monitoring of the business relationship and the transactions and carry out regular updates of their customer records. The implementation of appropriate processes and the taking of appropriate action is not only necessary in order to identfy transactions of relevance under sanctions law, but also in order to identify acts of circumvention and to prevent transactions related to these from being carried out. Appropriate awareness training is being conducted with the employees of the institutions.

Supervisory measures:

The OeNB is in regular contact with the financial sector, exercises its authority to solicit information (Art. 8 para. 2 of the Sanctions Act 2010) and is also consulted in connection with the assessment of matters that may be of relevance under sanctions law. The provision of information and guidelines for compliance with sanction measures is considered to be in line with the common international standard.

Supervised institutions submit reports to the OeNB based on the specific applicable legislative requirements (as a rule, these are the various specific EU regulations), in particular information on frozen funds. The OeNB may grant exemptions within the scope of its legal authority, e.g. with regard to the release of frozen funds.

In the course of on-site audits in the area of financial sanctions, an assessment is done to determine to what extent the systems deployed at the audited credit institution are fit for ensuring compliance with the provisions of foreign exchange and sanctions law. In addition to the organisational measures (structural and procedural organisation), the IT systems and their use are subjected to a detailed examination. This includes, in particular, the audited institution’s systems for monitoring of transactions and ongoing monitoring of the entire customer base. In the context of spot-check individual audits, transactions and customer relationships are evaluated with regard to issues of relevance under sanctions law. Such individual audits focus on the complete and up-to-date documentation on the client itself,

but also on the transaction in question. Depending on the business model, the institution's documentary credit and guarantee business, the currency exchange offices and precious metal business and the collaboration with payment service providers are also included in the on-site visit.

Exchange of information:
Dialogue regarding best practices as well as the revision and implementation of common guidelines to ensure the effective and uniform implementation of EU sanctions rules is undertaken at the EU level and has proven in practice to be an important interpretative aid for both institutions and supervisory bodies. The power to exchange information with the FMA provided for in Art. 3 para. 4 Financial Markets Anti-Money Laundering Act [FM-GwG] should be mentioned as an important example of enhancing the cooperation of the relevant national authorities.

Overall risk

Especially in light of the possibilities available to identify sanctioned persons, organisations or entities, freeze funds and prevent transactions in violation of the sanctions rules, the risk of sanctions violations can be significantly reduced. In addition, the FATF generally recognises that the financial sector has a good understanding of the threats and risks in the relevant compliance areas. Notwithstanding this, however, there is an inherent risk that institutions may be abused to circumvent sanctions against terrorist financing. The overall risk of this is classified as lowly to moderately significant.

Recommendations

In view of the possible challenges in connection with cross-border transactions, it would appear advisable to encourage (cross-border) dialogue between authorities.

Sector risk assessment - Lawyers

Sector of the legal profession

General information

1.1. Number of professionals

In Austria, there were **6,605 lawyers** and **2,270 trainee lawyers** as of 31 December 2020.

1.2. Practice areas (proportionate breakdown by practice area)

A lawyer acting as advisor, counsel or representative for his clients in all their public and private affairs is active in the following practice areas:

- Representation before the civil courts / arbitration tribunals and advising clients on initiating or avoiding civil proceedings (27.6%),
- Representation before the criminal courts and in criminal investigations (6.5%),
- Representation before administrative authorities and advising clients on administrative procedures (9.8%),
- Representation and advice in family law matters (8.5%),
- Representation and advice in inheritance law matters and questions of estate succession (6.1%),
- Involvement in the planning and implementation of transactions for the purchase or sale of real estate or businesses (19.5%),
- Assisting with planning and implementation in managing money, securities or other assets, opening or managing bank, savings or securities accounts (1.6%),
- Assisting with planning and implementation in forming, operating or managing trusts, companies, foundations or similar structures, including raising the funds necessary to form, operate or manage companies (6.3%), and
- other activities (14.1%, including representation of persons subject to guardianship, insolvency administration, debt collection, organisation of the law firm).

Pursuant to the results of a representative survey among the members, in which, inter alia, respondents were queried as to the ratio of their practice in each of the above-referenced practice areas, approximately 27% of the lawyer's practice areas involve transactions which are vulnerable to money-laundering; in 73% of the practice areas, there is no connection to transactions which are vulnerable to money laundering.

1.3. Law firm structure

The majority of lawyers work in very small entities. Half of all lawyers work as sole practitioners. Another quarter of the lawyers work in small entities consisting of up to three lawyers.

1.4. Specific characteristics of the legal profession

Lawyers have particularly strict training and admission requirements. The basic requirements for working as a lawyer are the completion of a degree in Austrian law at a university and five years of practical professional training, of which at least seven months must be spent at a court or a public prosecutor's office and at least three years in a lawyer's office. During this professional training period, prescribed training courses on a wide range

of subjects must be completed. Only after the trainee lawyer has passed the bar examination and after a positive assessment of his reliability has been furnished is the authorisation to practise as a lawyer granted by sovereign act.
The particularly rigorous training ensures a high level of expertise and professional experience, making the lawyer an excellent advisor, counsellor or representative for his clients in all their public and private affairs. A lawyer is also obliged to undergo continuous training and further education.
The nine Austrian regional Bars are responsible for safeguarding the honour, reputation and independence of the legal profession as well as for safeguarding the rights and supervising the obligations of lawyers. The regional Bars are thus empowered to issue recommendations, advice or instructions to lawyers in matters of professional law in order to safeguard the honour and reputation of the legal profession, but also to ensure compliance with professional ethics.
The disciplinary council of each regional Bar is exclusively responsible for adjudicating on professional misconduct. The appellate instance in disciplinary cases is the Austrian Supreme Court.
A lawyer is subject to supervision and discipline by the regional Bar under whose district he practices. A breach of professional ethics may lead to disqualification from practising as a lawyer.

1.5. General professional duties of care and their enhanced application in the area of ML/TF

A lawyer is required to carry out an individual analysis and assessment of the risk of his legal practice, taking into account his specific practice area as well as the type and size of his law firm and taking into account certain risk factors. In doing so, he must examine whether and to what extent, based on the structure of his law firm, his clients and the services he offers to his clients, he or his employees might be subject to exploitation for money laundering purposes. The risk assessment at the EU level and the National Risk Assessment should be taken into account.
The lawyer should record the assessment carried out and its results in writing and regularly update / verify the results to ensure that they are up to date.
Based on his internal firm risk assessment, the lawyer must implement and maintain adequate and appropriate policies and procedures to satisfy the due diligence obligations incumbent on him in the area of combating money laundering and terrorist financing with regard to parties, suspicious transaction reports, record-keeping, internal controls, risk assessment and risk management, as well as to ensure compliance with the relevant legal rules and to safeguard the channels of communication within his firm in order to prevent and avoid transactions related to money laundering or terrorist financing. The lawyer must take appropriate measures to familiarise himself, trainee lawyers and other employees with the rules aimed at preventing or combating money laundering and terrorist financing.
Irrespective of whether a transaction which is vulnerable to money-laundering within the meaning of Art. 8a para. 1 Lawyer's Act [German acronym: RAO] is involved, a lawyer is also obliged to establish the identity of the person for whose account the funds are held (Art. 9a RAO and Art. 43 Guidelines for Practising the Profession of Lawyer [RL-BA]) and to disclose this to the credit institution in the case of every fiduciary transaction (Treuhandabwicklung) (undertaken as a surrogate for the concurrent performance principle) that is handled through an escrow account. This obligation also applies to transactions that are not vulnerable to money-laundering.

1.6. Duty of confidentiality (legal privilege)

Lawyers are independent representatives and advisors whose obligations and responsibilities are solely to their clients. They also safeguard and defend the rights of the individual against the state and take action to enforce them. At the heart of the special relationship of trust between lawyers and their clients is professional confidentiality of lawyers enshrined in law, which is the basis for their professional independence and freedom from conflicts of interest.

According to the case law of the ECHR, the lawyer has a special status. He is entitled to special protections when communicating with a client. Any interference with such privileges must be provided for by law and must be justified and proportionate in a democratic society. However, professional secrecy and the lawyer's duty of confidentiality are indispensable in the light of the requirements of Articles 8 and 6 ECHR: the protection of professional secrecy constitutes a necessary guarantee for effectively safeguarding the right to a fair trial.

Pursuant to Art. 9 para. 4 RAO, in the case of one of the transactions listed in Art. 8a para. 1 RAO, the lawyer must provide the Federal Minister of the Interior (Criminal Intelligence Service, Financial Intelligence Unit pursuant to Art. 4 para. 2 Criminal Intelligence Service Act), upon request, with information on all circumstances known to him, to the extent that this is necessary to investigate a suspicion of money laundering (Art. 165 Austrian Criminal Code [StGB]) or terrorist financing (Art. 278d StGB) directed against the party.

The provisions of Art. 8a *et seq.* RAO govern the due diligence measures incumbent on every lawyer in order to ensure that he and his law firm prevent their being exploited for money laundering at the earliest possible stage. If a lawyer participates in a transaction in which the funds originate from a criminal predicate offence within the meaning of Art. 165 StGB, this not only constitutes a breach of professional ethics, it may also render the lawyer liable to prosecution (money laundering (Art. 165 StGB)); the same applies to participation in terrorist financing (Art. 278d StGB).

As stated above, it should be noted that not all legal work is relevant to ML/TF. The majority of the fields of legal practice are indeed not vulnerable to money laundering. This includes, for example, representation of clients before civil courts / arbitration panels and the provision of advice in relation to the initiation or avoidance of civil proceedings, representation before the criminal courts and in criminal investigations, representation of clients before administrative authorities and advice in relation to administrative proceedings, representation and advice in family law matters, representation and advice in inheritance law matters as well as the drafting of contracts in respect of transactions that are not vulnerable to money laundering.

Sector / Product / Service / Activity

The following list relates to the following ML/TF-vulnerable products/services in accordance with the catalogue of transactions defined as vulnerable to money laundering pursuant to Art. 8a RAO:

- Purchase or sale of real estate (including settlement by escrow)
- Purchase or sale of companies (including settlement by escrow)
- Management of money, securities or other assets
- Opening or managing bank, savings or securities accounts
- Formation, operation, management of trusts, corporate entities, foundations or similar structures, including raising the funds necessary for the formation, operation or management of entities.

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

General description

In the case of the purchase or sale of real estate, the areas of a lawyer's activity includes, *inter alia,* contract negotiations with the parties, preparation of the purchase agreement, the fiduciary ("documents v payment") settlement of the exchange of consideration to be tendered by both parties, the preparation of a self-assessment tax return, the obtaining of any necessary permits (land transfer authority, forestry, property subdivision, zoning, etc.) and the execution on the land registry.

In cases of the purchase or sale of corporate entities, the lawyer's activities include, *inter alia,* contract negotiations with the parties, the drafting of contracts, the drafting of articles of association, the fiduciary ("documents v payment") settlement of the purchase price payment and the transfer of shares or assets, including the further acts of implementation, in particular the obtaining of any necessary permits (land transfer authority; approval by the Cartel Court; approval under the Foreign Trade Act [AußWG], etc.), the preparation of a self-assessment tax return and the implementation on the commercial register.

The administration of money, securities or other assets is regularly carried out by lawyers acting in the capacity of (court-appointed) guardians and insolvency administrators. Other than in these instances, a lawyer administers financial assets almost exclusively in the context of settlement escrows in connection with the purchase and sale of real estate or corporate entities.

The opening or management of bank, savings or securities accounts is generally carried out by way of settlement escrows in connection with the sale of real estate and company shares, or in certain cases where the lawyer is acting as a constitutive officer or director of an entity.

Within their practice areas, lawyers act in connection with the formation and operation of companies and private foundations. Furthermore, as members of the executive bodies of private foundations (boards of trustees, advisory board), lawyers participate in managing and administering the foundation's assets, including the payment of benefits to beneficiaries; lawyers also perform supervisory board functions in companies and perform oversight of management by the board of directors.

Threat

Terrorist financing:
In the SNRA, the threat of lawyers' services being exploited for terrorist activities was classified as very significant and it was stated that the assessment of the TF risk in connection with legal services of lawyers is considered in connection with the ML area; applying this systematic analysis, the Austria-specific risk situation for both areas shows that not only the structure of the legal profession in Austria and the supervisory regime applied, but, and in general, the enhanced attention given to the area of counter-terrorism, especially more recently, leads to the conclusion that the country-specific threat situation in Austria appears to be mitigated as compared to the classification which was assigned in the SRNA.

Conclusion:
The threat in the area of terrorist financing should be classified as moderately significant.

Money laundering:
Lawyers have a special position of trust in society. The involvement of a lawyer or the handling of the transaction through him is sometimes intended to signal credibility, creditworthiness, legitimacy and respectability.

Criminals may seek to create complex or opaque structures involving many jurisdictions, particularly offshore jurisdictions with secret chains of ownership where the owner of another company or legal structure is registered elsewhere. Through this combination of legal services, criminals may seek to add complexity to the transaction.

There is an increased potential risk of money laundering in the acquisition of real estate or companies and shares in companies by persons domiciled or resident outside the EU/EEA. At times, purchaser entities acting as buyers, which are often only set up for the purpose of the specific acquisition, may be owned by multilevel legal entities in complicated nested structures, with the result that it proves very difficult to identify the beneficial owners or the origin of the funds, even within Austria. The same applies to cases of the formation of (buyer) entities for the purpose of managing assets (such as equity holdings).

The threat scenario in connection with the opening and management of bank, savings and securities accounts or of trusts, foundations and similar structures by lawyers appears to be less heightened overall, especially since lawyers' awareness of the sensitivity of such transactions has meanwhile increased considerably, especially when such tasks are handled by legal professionals working in Austria, as compared, for example, with the international transaction business.

Conclusion:
Just as in the case of terrorist financing, the professional and general economic environment mean that the threat should be classified as moderately significant.

Vulnerability

Terrorist financing:
The assessment of vulnerability to terrorist financing in the context of legal services provided by lawyers is generally considered in conjunction with money laundering schemes designed to conceal the illicit origin of funds.

However, it should be noted that there is only a small probability that the purchase or sale of real estate will be exploited for the financing of terrorism. In any case, there would have to be additional elements present, such as the transfer of the proceeds of the sale to dubious associations, countries or persons. As a rule, however, these are not transactions where lawyers are involved.

The involvement of a lawyer in the purchase and sale of companies for the purpose of terrorist financing is also rather atypical, since terrorist financing usually requires quick liquid funds and therefore long-term investments in companies are not suitable for the purpose of terrorist financing. In the case of corporate transactions, in any case, there would have to be additional circumstances present, in particular with regard to the transfer of sales proceeds to corresponding payees, however, these are not transactions where lawyers are involved and/or they can no longer be classified as (typical) corporate transactions.

Conclusion:

Based on the SNRA, which suggests moderately significant vulnerability, the framework conditions presented lead us to class the vulnerability of lawyers to exploitation for the purposes of terrorist financing as lowly significant.

Money laundering:

In the SNRA summary scenarios, the vulnerability of lawyers with regard to exploitation for purposes of money laundering was classified as significant. In the text which follows, we will analyse the national vulnerability.

(a) Risk exposure:

As lawyers are often organised and operate within small structural units, perpetrators may see an opportunity for a lack of sensitivity and vigilance to ML risks. It may also be that lawyers are involved in the management of complex legal situations and client behaviour triggers as-yet unknown red flags.

(b) Risk awareness:

The regional Bars are obliged to verify their members' compliance with the provisions of Art. 8a *et seq.* RAO and take a variety of steps in monitoring the ML/TF obligations of their members. During on-site visits, regional Bars check whether lawyers, trainee lawyers and law firm staff comply with the legal rules regarding the prevention of ML/TF. Within the scope of a client money or fiduciary audit, compliance with other legal provisions (e.g. regarding beneficial ownership) is also examined. Among other things, such audits examine whether a written law firm risk analysis is in place and what strategies have been developed to prevent ML/TF (e.g. law firm guidelines, staff training, designation of an anti-money laundering officer, etc.). On average, about 20 % of all lawyers were audited annually over the last four years.

In the course of the on-site audits, regional Bars inquire *inter alia* into whether the identity of the parties and the beneficial owner of money laundering transactions has been established and documented, whether suspicious transaction reports have been filed and whether the corresponding documentation is in place. These audits are carried out on a random basis as well as on an *ad hoc* basis if there are any suspicious circumstances present. The audit results show that, to the greatest extent, the legal requirements are complied with and, in particular, that the identification of beneficial owners is carried out in a practically flawless fashion.

On the basis of these findings, it is clear that there is a high level of risk awareness in the legal profession.

(c) Legal environment and supervision/governance:

The fact that, in addition to the lawyer, other obliged entities and authorities are regularly involved in the conclusion and settlement of a transaction does not, as a rule, entail neglect of the obligations incumbent on lawyers to prevent money laundering and terrorist financing, but rather it has the consequence that special attention is paid to these obligations. This is because negligence in discharging one's own obligations entails not least of all the considerable risk that this will come to light when the obligations are independently fulfilled by another person/entity involved in the system of combating money laundering and terrorist financing (such as a credit institution), and as a consequence there is a risk of considerable disadvantages to a lawyer who neglects his obligations. The same applies to the supervision exercised by the regional Bar, in view of which every lawyer is aware that money laundering audits should always be expected. This also increases the sensitivity in this area considerably.

For example, in the case of real estate transactions, an entry in the court's land registry is required. In addition, lawyers must handle the calculation and payment of capital gains tax on property, real estate transfer tax and registration fees and file the corresponding reports with the tax authorities.
This self-assessment by the representatives of the parties is also in the interests of the tax administration, whose workload is considerably lightened as a result. The tax authorities then examine whether the self-assessment has been carried out correctly by means of special audits (external audits).
In the case of real estate transactions involving buyers from third countries (acquisition of land by aliens), the authorities also conduct a check of the beneficial owner. It is particularly significant that the flow of payments, insofar as they occur - as is usually the case - via bank accounts, is also (and especially) checked by the banks; in addition, settlement of funds transactions are handled via the escrow entities of the regional Bar, which are empowered to audit them as part of their oversight duties.

Finally, a real estate transaction requires notarisation, during which the notary carries out an additional verification of the identity of the persons involved.

The legal framework in Austria is in line with the current status of the AMLD. Compliance with organisational measures (in particular risk assessments, training and structured processes) in law firms ensures that ML/TF risks are adequately taken into account in the course of accepting new clients, taking on mandates and managing ongoing business relationships.

Supervision of the legal profession in the realm of ML/TF is carried out by the nine regional Bars, which conduct regular as well as *ad-hoc* checks. Their supervision includes not only a review of individual mandates, but also the law firm's compliance with prescribed organisational measures. Violations can result in far-reaching disciplinary sanctions.

Human and financial resources:
In the nine regional Bars, a total of 146 persons were involved in supervision related to the prevention of ML/TF in 2020.

Conclusion:
Based on the SNRA summary scenarios, which suggest significant vulnerability *per se*, the framework conditions presented lead us to classify the vulnerability of lawyers in Austria to exploitation for purposes of money laundering as moderately significant.

Risk-mitigating measures

- In addition to the risk-mitigating measures already referred to above, the following measures should also be noted, which would further reduce the risk in future:
- Increased individual case assessments and a risk-based audit approach by the regional Bars: It is important to increasingly incorporate the analyses and assessments of risk analyses by individual professionals into the regional Bars' supervision, both in terms of substance and in organisational respects,
- in the area of further training, as well, the findings derived from supervisory activities should be incorporated in a targeted way,
- strict disciplinary consequences for violations of professional ethics rules,
- law firm-specific risk assessment and mandate-specific review,
- increased networking and cooperation with other agencies and obliged entities: First and foremost, the FIU (Financial Intelligence Unit) and the register of beneficial

owners, which has already been set up. Lawyers are entitled to inspect the register according to Art. 9 Beneficial Owners Register Act [WiEReG]. In particular, the findings derived from networking with the FIU should be directly incorporated into informational documents provided to lawyers or in training courses,
- in addition, professionals must be referred to the security tools associated with the escrow trusts (trust register, settlement via recognised credit institution).

Overall risk

The overall risk should be classified as moderately significant.

Recommendations

- Continuation of training and further education measures,
- increased conduct of off-site audits by regional Bars,
- more up-to-date information from the FIU on methods of money laundering and terrorist financing and on criteria enabling suspicious transactions to be recognised

Sector risk assessment – Notaries

Notaries

General information

1.1 General

As of 31 October 2020, there are 522 authorised notarial positions, with 519 notaries and 582 notarial candidates in Austria. Around 76% of these notary's offices are run as sole-practitioner notarial offices and around 24% of them as partnerships. The notary's practice area ranges from providing legal advice, to ascertaining the intent of parties and certifying documents, to performing activities on behalf of the state. As a basic principle, Austrian notaries are generalists. This means, first, that each notary can provide the same legal services and thus covers all of the practice areas described below, and second, that a notary is *per se* permitted to practice throughout the entire federal territory of Austria. The legally defined sphere of activity of a notary includes the following:

Drafting of official documents; drafting of private deeds/representing parties; escrow or trust settlement; mediator; service as commissioner of decedents' estates.

1.2 Practice areas

Acting within their legally defined remit, notaries perform activities in various practice areas. The breakdown of notarial practice areas by turnover (in %) is as follows:

a. Involvement in planning or implementation of **the purchase or sale of real estate**, including settlement escrow: 28.8 %.
b. Involvement in planning or implementation of **the purchase or sale of companies**, including settlement escrow: 6.6 %.
c. Involvement in planning or implementation of the **management of money, securities or other assets**, the opening or management of bank, savings or securities accounts in the context of **trusteeship work**): 0.8%.
d. Involvement in planning or implementation of the **management of money, securities or other assets**, the opening or management of bank, savings or securities accounts as a **health care proxy or legal guardian**: 0.7%.
e. Involvement in planning or implementation of the **management of money, securities or other assets**, the opening or management of bank, savings or securities accounts in **other cases**: 0.6%.
f. Involvement in planning or implementation of the **formation of companies or foundations,** including the raising of funds necessary for formation, operation or administration of companies and related trusteeships: 8.7%.
g. Involvement in the **operation or administration of companies or foundations,** including the procurement of funds required to operate or administer companies, e.g. as part of appointment to a board of directors: 0.8%.
h. Involvement in planning or implementation of the **formation, operation or administration of trusts or similar structures**, including the raising of funds necessary for their formation, operation or administration: 0.2%.
i. **Service as a commissioner** in **probate matters**: 21 %
j. **Service as a commissioner** with regard to inspection of **company register and land registry**: 3.9%

k. Provision of representation and advice in **family law matters** (e.g. adoption, the law governing reproductive medicine, ante- and post-nuptial agreements): 4.4%.
l. Provision of representation and advice in **inheritance law matters**: 11 %
m. Activities in the field of **pension provision**: 7.5%.
n. Representation of clients before **civil courts / arbitration tribunals / criminal courts** and advice with regard to initiating or avoiding proceedings: 0.3%.
o. Representation of clients before (**administrative) authorities** and advice in relation to administrative procedures: 1.4%.
p. Service as a **mediator**: 0.1
q. **Other activities**: 3.3

47.2% of the notarial practice areas involve "transactions vulnerable to money laundering" as defined in Art. 36a Notarial Code [German acronym: NO] (see section 1.2. a. to h. above); in 52.9% of notarial practice areas, there is no connection with transactions that are considered vulnerable to money laundering (see section 1.2. i. to q. above).
An analysis of notary clientele (trustors) by domicile for 2019 reveals that clients were predominantly from Austria (95.96%) or the EU/EEA and Switzerland (3.85%). Parties from "other countries" (not specified here) account for a share of 0.19%. Those parties come, in particular, from the US, Canada, Australia, Liechtenstein and Bosnia and Herzegovina.
Only 0.001% of notarial clients in 2019 came from countries specified in the European Commission Delegated Regulation (EU) 2016/1675 (Afghanistan, Ethiopia, Bosnia and Herzegovina, Guyana, Iraq, Yemen, Laos, Pakistan, Sri Lanka, Syria, Tunisia, Trinidad and Tobago, Uganda, Vanuatu).
26.2% of notaries have clients who qualify as PEPs. 96.3% of these parties are domestic PEPs, 3.7% of them are foreign PEPs.
When the business relationship is being established or the transaction is being executed, 95.6% of the parties are physically present, 4.4% of cases are remote transactions (parties are not present).

1.3 Specifics of the notarial profession
The Austrian notary is a freelance legal practitioner who advises clients and prepares contracts and public documents/deeds. He is predominantly active in non-contentious and advisory legal fields and holds the official title of "public notary [*öffentlicher Notar*]". His work is distinguished, first and foremost, by the fact that he acts independently and exercises a partially sovereign role (e.g. as commissioner in performing substantive judicial tasks and preparing public documents/deeds). In contrast to lawyers, a notary (as a public office holder) has a duty to instruct all parties and to protect the interests of all parties involved in a legal transaction equally. Involvement in any kind of prohibited, suspicious or sham transactions is prohibited (Art. 5 para. 3, 34 NO).

When providing his services (products), the notary is subject to strict professional and disciplinary regulations and must ensure a high standard of care in the provision of his services in accordance with the provisions of the Notarial Code and guidelines of the Austrian Chamber of Notaries (hereinafter *ÖNK*).
Top-level supervision of the notarial profession lies with the Federal Minister of Justice, and the general supervision of notaries' official conduct lies with the presidents of the courts of first and second instance. General and direct professional supervision of notaries in their official activities, but also in their professional conduct, is the responsibility of the competent Chamber of Notaries (hereinafter CN, Art. 153 NO). For more detail of this, see section 2.2.2.

The creation, transfer and relocation of notarial positions is only possible by means of a Regulation of the Federal Minister of Justice ("systemisation").

Methodology

2.1 Products – services with relevance to ML/TF

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

1. *the purchase or sale of real estate or companies,*
2. *the management of money, securities or other assets, the opening or management of bank, savings or securities accounts, or*
3. *the formation, operation or administration of trusts, companies, foundations or similar structures, including the raising of funds necessary for the formation, operation or administration of companies.*"

This broad definition of transactions "vulnerable to money laundering" covers large parts of the activities of notaries, particularly in the realm of financial and real estate transactions. Overall, the share of activities relating to transactions "vulnerable to money laundering" within the notarial profession is 47.2% (for more detail of this, see section 1.2. a. to h.).
The remaining 52.8% of notarial services (for more detail of this, see section 1.2. i. to q. above) either do not constitute transactions "vulnerable to money laundering" or are definitionally transactions "vulnerable to money laundering", but nevertheless pose no, or only very little, risk of ML/TF for various reasons.

2.2.1 The "settlement escrow"

The majority of transactions "vulnerable to money laundering" in which the notary is involved in a payment transaction are carried out by means of a notarial escrow (for the purpose of securing concurrent settlement by the notary to protect the interests of the buyer and seller), which must be entered in the trustee register [*THR*] of the Austrian Chamber of Notaries (ÖNK) for escrow amounts of € 10,000 or more. In practice, the escrow product is almost always associated with real estate and corporate law transactions that are vulnerable to money laundering.
Number of registrations on the THR: in 2017 43,435; in 2018 44,591; in 2019 48,156.
The average annual amounts (total amounts) of escrow were: in 2017 EUR 259,526; in 2018 EUR 278,625; in 2019 EUR 295,716.
The average number of trustors involved in an escrow was as follows: 2017 2.97; 2018 2.99; 2019 3.02.

At **Notartreuhandbank AG** (NTB), currently the only credit institution authorised and recognised to handle notarial escrow, the following escrow accounts were opened by notaries: 2017: 41,594; 2018: 42,556; 2019: 53,268, opened for an average duration of 4 months and 21 days in 2019. NTB maintains only escrow accounts in the names of notaries, which must comply with the strictest transparency and security requirements established by law and guidelines (in particular THR 1999). Notaries are not allowed to open accounts with NTB for their own business.

2.2.2 Audits, training and information measures

The CNs are obliged to regularly audit the files, business registers, books, directories, rolls and business operations of notaries as a whole (Art. 154 para. 1 NO, "Audit"). In particular, the CNs must monitor notaries' compliance with the provisions that serve to prevent or

combat money laundering or the financing of terrorism (hereinafter ML/TF). In suspicious cases, the CN will also perform unannounced interim or special audits (extraordinary audit). If the CN finds a deficiency or violation in the course of the audit or on another occasion, then - depending on the severity – it will issue an appropriate official reminder, conduct administrative penalty proceedings or initiate disciplinary proceedings before the Higher Regional Court as disciplinary court. If the CN discovers circumstances that relate to ML/TF, it must also submit a suspicious transaction report to the Financial Intelligence Unit (Art. 36c para. 1 NO). On average, each notary's office is audited at least once every 3 to 5 years (in 2017 there were 77 office audits nationwide, in 2018 there were 245 office audits nationwide and in 2019 there were 86 office audits nationwide).
The ÖNK offers numerous seminars on the topic of preventing and combating ML/TF, which are in high demand: 5 seminars were held in 2017, 10 seminars in 2018 and 10 seminars in 2019. Since 2008, the ÖNK has also provided its members with a continuously updated code of practice on the topic of ML/TF ("Recommendations of the ÖNK on the prevention of ML/TF") in electronic form and informs its members regularly and on an *ad hoc* basis about important new developments in this area by means of circulars and mailings.
48.2 % of notary's offices conduct in-house training/instruction on these topics several times a year, 43.6% of notary's offices at least once a year and 6.2% less frequently than that. Around 60% of notaries, around 80 % of notarial candidates, around 26 % of other legal staff and around 92% of non-legal staff receive training. In addition, around 68% of notary's offices conduct external training on the topic of preventing ML/TF, in which around 91% of notaries, around 86% of notarial candidates, around 8% of other legal staff and around 21% of non-legal staff receive training.

Product-specific risk assessment

Non-financial products, item 10 "Legal services from notaries and other independent legal professions" of SNRA SWD (2019) 650 (page 182 *et seq.*, hereinafter "legal services").

General description

According to Art. 2 para. 1 item 3 letter b of Directive (EU) 2018/843 and the Supranational Risk Assessment (SNRA, page 186), notarial services in Austria include the following areas (transactions vulnerable to money laundering pursuant to Art. 36a NO): purchase/sale of real estate, purchase/sale of companies, management of money, securities or other assets, opening or management of bank, savings or securities accounts and formation, operation and management of trusts, companies, foundations or similar structures including procurement of the funds required for the formation, operation or management of companies. In line with SNRA SWD (2019) 650, these services are subsumed under Non-Financial Products, item 10 "Legal services from notaries and other independent legal professions" (hereinafter "legal services") of SNRA SWD (2019) 650 (page 182 *et seq*.); for better understanding, the services are summarised separately below by individual area.

Purchase/sale of real estate: Within their remit under both Art. 1 NO and Art. 5 NO, notaries are involved in their clients' acquisition of real estate (providing legal advice, preparing contracts, notarising signatures, executing transactions on the land registry, assessment and collection of fees under tax law). This notarial practice area comprises 28.8% of their activity (see section 1.2. a. above).

Purchase/sale of companies: Within their remit under both Art. 1 NO and Art. 5 NO, notaries are involved in their clients' acquisition of companies (providing legal advice, preparing contracts, notarising signatures, assessment and collection of fees under tax law). In total, the share of these notarial services comes to 6.6% (see section 1.2.b. above).

Administration of money, securities or other assets: The administration of money, securities and other assets by notaries is, in principle, possible under Art. 5 NO, but it is rare, which is shown by the low proportion of 2.1% of notarial activities in this area (see sections 1.2.c., d. and e. above). In practice, the administration of money, securities and other assets by the notary takes place predominantly (with a share of 1.5 %) as a court-appointed trustee or as part of a notary's service as a (court-appointed) legal guardian or authorised caregiver for persons lacking the capacity to make decisions.

Opening or managing bank, savings or securities accounts: Notaries may open bank accounts, in particular in connection with the purchase/sale of real estate and the purchase/sale of companies, but the accounts in these cases are always fiduciary accounts (escrow accounts) for the settlement of the transaction in question. There is a tightly monitored professional and supervisory network for these accounts, which may only be held at a credit institution specifically recognised for this purpose (see section 2.2.1 above). Furthermore, it is possible for a notary to open or manage bank, savings or securities accounts in the context of managing money, securities or other assets. In this case, these are generally accounts that are managed by the notary as a trustee or legal guardian and they are therefore subject to judicial supervision. Finally, it is possible for a notary to open a bank account in the context of holding funds in safekeeping (Art. 5 and Art. 104 *et seq.* NO). Accounts under Art. 104 NO (accounts which can only be opened in connection with the recording of a notarial deed for the safekeeping of money and subsequent delivery by directions of a party to a specific recipient or for deposit with the authorities or with the court) are usually opened in order to deposit funds with the court and are therefore of no interest to offenders. They hardly play any role in practice.
Beyond the points mentioned, notaries ordinarily have no involvement in the opening or management of bank savings or securities accounts.

Formation, operation, administration of trusts, companies, foundations or similar structures including raising the funds necessary for the formation, operation or administration of companies: "Trusts" are foreign to the Austrian legal system. In Austria there are foundations under the Private Foundation Act (PSG). Pursuant to Art. 1 para. 1 Private Foundations Act [PSG], private foundations are legal entities to which assets have been dedicated by their founder in order to achieve a permitted purpose determined by the founder, through their use, administration and realisation; private foundations have legal personality and must have their seat in Austria. Private foundations must also be entered on the commercial register and on the Register of Beneficial Owners. Within their remit under both Art. 1 NO and Art. 5 NO (and on the basis of legal requirements of form), notaries are involved in forming companies and foundations for their clients (providing clients with legal advice, drafting and, if necessary, amending the articles of association, filing of applications with the commercial register, asssisting with any restructuring). In total, the share of this activity amounts to 9.7 % (see sections 1.2. f., g. and h. above).
Notaries are not usually involved in the administration or operation of companies or similar structures. Notaries are also not involved in raising the funds necessary to form, operate or manage companies or similar structures.

Threat

Terrorist financing:
Under the SNRA summary scenarios, the threat of abuse of legal services is generally classified as very significant for both the area of terrorist financing and the area of money laundering due to the identified methods for concealing the illicit origin of financial resources (see SNRA SWD (2019) 650, page 183). This assessment does not appear to hold

true, since in the case of money laundering the assets in question are always obtained through criminal acts (predicate offences), but in the case of terrorist financing the assets can come from both legal and illegal sources (and accordingly the focus is primarily on the use of the funds). A differentiated, separate consideration of the areas of terrorist financing / money laundering and of transactions vulnerable to money laundering within the meaning of Art. 2 para. 1 item 3 letter b of Directive (EU) 2018/843 and the Notarial Code is therefore sensible and is undertaken below.

In all practice areas which are vulnerable to money laundering, the **threat** of abuse for terrorist financing lies in the fact that the involvement of a notary or the handling of the transaction via the notary could suggest credibility, respectability and creditworthiness. If bank accounts are involved, there could also be a risk that banks will not check notaries as strictly as account holders.

A **classic threat scenario** in the **purchase/sale of real estate** might, for example, be an attempt by perpetrators to generate assets for purposes of terrorist financing through investments in the real estate sector (e.g. by making profitable investments).

When **buying/selling companies, a classic threat scenario** might, for example, be the attempt by perpetrators to generate assets for purposes of terrorist financing through investments in companies (e.g. by making profitable investments).

A **classic threat scenario in the management of money, securities or other assets** could be the attempt by perpetrators to use notaries as "straw men" in the management of assets for the purposes of terrorist financing.

A classic threat scenario in the area of terrorist financing when **opening or managing bank, savings or securities accounts** might, for example, be the opening of donation accounts as a cover to collect funds.

A classic threat scenario in the **formation, operation and administration of trusts, companies, foundations or similar structures, including the procurement of funds required for the formation, operation or administration of companies,** might, for example, be the attempt by perpetrators to obtain money from companies in formation**,** which is subsequently to be used for the purposes of terrorist financing.

Conclusion:
In summary, the threat in the area of terrorist financing should be classified as lowly significant.

Money laundering:
In all of the practice areas which are vulnerable to money laundering, the **threat** of exploitation for money laundering lies in the fact that the involvement of a notary or the processing of the transaction via the notary could suggest credibility and respectability. If bank accounts are involved, there could also be a risk that banks will not check notaries as strictly as account holders.

A **classic money laundering threat scenario** in connection with the **purchase/sale of real estate** might, for example, be the attempt by perpetrators to disguise the origin of ill-gotten assets by investing in the real estate sector. Especially in the case of high-priced real estate,

the illegal origin of large sums of proceeds from criminal activities could be concealed "at a stroke" and thus "laundered clean".

A **classic money laundering threat scenario** in connection with the **purchase/sale of companies in** the money laundering sector might, for example, be the attempt by perpetrators to disguise the origin of ill-gotten assets by acquiring companies. Especially in the case of company acquisitions involving large amounts, the illegal origin of large sums of proceeds from criminal activities could be concealed "at a stroke" and thus "laundered clean". Through such investments, the creditworthiness of acquired companies could also be used for further criminal activities (e.g. by taking out loans).

A **classic money laundering threat scenario in connection with the administration of money, securities or other assets** might, for example, be the attempt by perpetrators to use notaries as "straw men" in the administration of assets to disguise the origin of the funds.

A **classic money laundering threat scenario in connection with opening or managing bank, savings or securities accounts** might, for example, be the attempt to exploit notaries as financial agents by making financial transactions through accounts in order to conceal the illicit origin of the funds.

A **classic money laundering threat scenario in connection with the formation, operation and administration of trusts, companies, foundations or similar structures, including procurement of the funds required for the formation, operation or administration of companies,** might, for example, be the attempt by perpetrators to use incriminated assets for formation of corporate entities as a means of concealing the illegal origins of those assets.

Conclusion:
In summary, the threat of money laundering should be classified as moderately significant to significant.

Vulnerability

In the SNRA summary scenarios, the vulnerability of legal services for the area of terrorist financing and the area of money laundering is uniformly classified as significant. Since there are no substantive differences in the notarial sector with regard to risk exposure, risk awareness and legal framework/supervision/governance, a uniform assessment on vulnerability is given here, as in the SNRA.

(a) Risk exposure:
In the areas of purchase/sale of real estate and purchase/sale of companies, notaries handle large numbers of transactions every year, some of which involve high monetary amounts (see section 2.2.1, page 3 above). In addition, the COVID 19 pandemic is currently causing real estate prices to rise, in some cases sharply. Overall, Austria is "popular" with criminals also because of its humane prison conditions, which could increase the risk of criminal activities.

(b) Risk awareness:
There is a high level of risk awareness throughout the profession (notaries, notarial candidates, employees and chambers), thanks in particular to the large number of risk-mitigating measures: every notary is obliged to prepare and continually update a personal risk assessment. The ÖNK also regularly prepares a sectoral risk assessment for the

notarial sector, which, like the National and Supranational Risk Asessments, is incorporated by reference in the notary's personal assessment. The ÖNK and the chambers of notaries as supervisory authorities undertake comprehensive measures in the area of training and awareness-raising (seminars, detailed and continually updated guidance notes, information letters, information provided on the notar.at website, etc). Regular and effective supervisory measures are undertaken by the chambers of notaries (chambers audits pursuant to Art. 154 NO), in which the chambers audit notaries' compliance, in particular, with their obligations under ML/TF law. Where violations of professional ethics rules are found, there are strict disciplinary consequences (see Art. 158 NO). In addition, in this area, particular attention must be paid to the security instruments associated with the settlement escrow (such escrows exist in practically every real estate transaction and in most corporate transactions) (trust register, settlement via a recognised credit institution pursuant to Art. 109a NO). See sections 2.2.1 and 2.2.2 above for more detail, pp 3-4.

(c) Legal framework and supervision/governance:
In addition, it should be noted that in Austria, notarial services involve not only the notary but also other professional groups, authorities and courts that have an obligation to prevent money laundering and terrorist financing. For example, in the case of real estate transactions, an examination of the underlying titles (deeds) is carried out by the land registry courts (Art. 26 Land Registry Act [GBG]) before entry on the court's land registry. The tax authorities are involved with their audit mechanisms, in particular as the registry authority of the Register of Beneficial Owners and in connection with the calculation and payment of taxes and fees (real estate income tax, land transfer tax, registration fee). Insofar as self-assessment is handled by notaries, this is done in the interest of the tax authorities, who then also verify returns by means of special audits; the notaries assume a quasi tax collection role for the Republic of Austria in this area. In the case of real estate transactions with buyers from third countries (acquisition of land by aliens), the authorities also examine the beneficial owner.

Every payment through bank accounts involves a bank, which in turn is subject to the strict regulations of the Financial Markets Anti-Money Laundering Act [FM-GwG]. In the case of notarial transactions, there is also a strict recognition procedure prescribing the banks at which notaries are allowed to hold accounts and deposit client funds. Currently, this is only Notartreuhandbank (NTB), which has to comply with a same-day notification system of all parties involved in a transaction, in addition to other security measures.

Human and financial resources:
In 2020, a total of 157 persons in the ÖNK, the six chambers of notaries and the Permanent Office in Brussels are involved in matters of preventing terrorist financing and money laundering as well as supervision in connection with the prevention of ML/TF.

Conclusion:
Based on the SNRA summary scenarios, which suggest significant vulnerability, the national and sectoral professional framework conditions (which are identical for the areas of terrorist financing and money laundering) described here lead us to classify the vulnerability of notaries to abuse for the purposes of terrorist financing or money laundering as moderately significant to significant.

Risk-mitigating measures

In addition to the risk-mitigating measures already noted above under Risk Awareness, the following future measures should be noted, which will also further reduce the risk in future:

- The chambers of notaries should should strengthen their risk-based approach in terms of their supervisory measures (e.g. risk classification of notaries by technical risk monitoring, on-site and off-site visits) by establishing a central staff unit at the ÖNK to coordinate the money laundering/terrorist financing supervisory measures by the chambers of notaries. More intense scrutiny of personal risk assessments is undertaken.
- The knowledge gained from risk-based supervision is increasingly being incorporated into training and further education; 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 located in Austria or another Member State) within the scope of application of the Beneficial Owners Register Act (BORA). If these foreign legal entities want to acquire ownership of a property located in Austria, they are considered foreign legal entities subject to the reporting requirement, and must be entered on the supplementary register for other legal entities before notarisation or recording of a notarial deed for purposes of acquiring a property located in Austria, and must then report their beneficial owners. In future, notaries must ensure that, prior to notarising or recording a notarial deed for purposes of the acquisition of real estate in Austria by foreign legal entities subject to the reporting obligation as well as trusts and arrangements similar to trusts whose management is not located within Austria or in another Member State, they have reported the beneficial owners. The obligations of the legal entities in question are enforced by means of high fines (penalties for tax offences of up to EUR 200,000).
- Increased cooperation (administrative assistance) between ÖNK/chambers of notaries and other stakeholders in the area of preventing money laundering or the financing of terrorism will further mitigate the risk. In particular, there is a PPP with the Federal Ministry of the Interior/Financial Intelligence Unit (A-FIU), which, for example, is required to provide notaries with access to up-to-date information on methods used by criminals and criteria for assessing these to provide notaries with timely feedback regarding the effectiveness of suspicious transaction reports and the measures taken in response (Art. 37 para. 9 NO).

Overall risk

Considering the measures already in place (see section on Risk Awareness) and the future risk-mitigating measures, the overall risk for terrorist financing should be classified as lowly to moderately significant and for money laundering as moderately significant.

Recommendations

- Continue the intensified cooperation between notaries' offices and other authorities involved, in particular the Federal Ministry of Justice, Federal Ministry of the Interior/Financial Intelligence Unit (A-FIU).
- Continue to train and raise awareness within the profession.
- Expand risk-based supervision, establishment of a staff unit at the ÖNK and train auditors in order to complement the necessary internal professional expertise with specialised know-how on preventing and detecting money laundering or terrorist financing.

Sector risk assessment – Chartered accounting professions

Tax consultancy and accounting

General information

The professional groups of tax advisors and accountants, as independent professions in the area of economic and legal advice and representation, fall into the category of the non-financial sector. With regard to the prevention of money laundering and terrorist financing, tax advisors and accountants primarily have an indirect "observer role", as they are rarely directly involved in financial transactions. For the most part, they only play a direct role in financial transactions when they act as trustees, but such services do not form part of the core activity of these professional groups.

However, through their activities and services, they gain detailed insights into their clients' business structures and finances. This is especially true with regard to companies. In this way, tax advisors and accountants are sometimes able to form a picture of the sources of income and on the beneficial owners, and any potential anomalies may be identified. Thus, they can also play an important role in preventing money laundering and terrorist financing. Pursuant to Art. 77 para. 6 Chartered Accountants' Act 2017 [WTBG 2017], tax advisors and accountants are entitled to regard the information provided to them and the documents handed over to them by their clients (in particular the numerical details) as correct and complete. Tax advisors and accountants may only perform audit mandates and other mandates requiring impartiality and independence after conscientiously ascertaining the accuracy of the facts and circumstances they are asked to verify.

Number of professionals and total turnover

As of January 2020, there are a total of 11,052 holders of professional licences in the fields of tax consultancy and accountancy in Austria.
This total breaks down further into 7898 natural persons and 3154 legal entities.
As of January 2020, there are a total of 8080 professional tax advisors in Austria. Of these, 5915 are natural persons and 2165 are legal entities.
As of January 2020, there are a total of 2972 holders of professional licences in the field of accountancy in Austria. Of these, 1983 are natural persons and 989 are legal entities.
The calculated total turnover of all tax advisors and accountants in Austria was around 2.8 bn euros as of 2019.

Firm structure

Tax advisors and accountants use a wide variety of firm structures to carry out their activities. These range from small one-person firms to large firm networks with as many as 1000 employees or more. Their employees are not only professionals and trainees, but also persons who perform front and back office tasks or who are employed in an organisational and system support capacity in the firms.
In 2019, the size of tax consultancy and accountacy firms in Austria breaks down by the number of employees as follows:

- around 70% - firms with fewer than ten employees
- around 26% - firms with 10 - 50 employees
- around 4% - firms with 50 - over 500 employees.

Number of clients

For the most part, tax advisors and accountants work for a large number of clients. Firstly, clients include private individuals from all professional areas and, secondly and importantly, they include companies from the widest variety of economic sectors.

The statistical distribution of the number of clients per tax consultancy and accountacy firm in Austria as of 2019 is as follows:

- around 41% of tax consultancy and accountacy firms serve up to 100 clients,
- around 42% serve up to 500 clients,
- around 11% serve up to 1000 clients,
- and around 6% of tax consultancy and accountacy firms even serve more than 1000 clients.

Duty of confidentiality (legal privilege)

Due to the strictly confidential relationship with their clients, tax advisors and accountants are subject to a duty of confidentiality within the scope of their professional activities. The exact rule and its wording can be found in Art. 80 WTBG 2017. However, pursuant to Art. 80 para. 4 WTBG 2017, this duty of confidentiality does not apply if and to the extent that reporting and information obligations apply under the provisions of Directive (EU) 2018/843 and the implementing measures issued in connection with that Directive.

Threat

Money laundering and terrorist financing:

As in the SNRA, the KSW would point out that the assessment of the terrorist threat in connection with services provided by accountants and tax advisors was examined together with money laundering. The terrorist financing risk therefore does not require a separate assessment.

In the SNRA summary scenarios, the threat of tax advisors and accountants being abused for money laundering and terrorist activities was rated as significant. In the text which follows, we will analyse the national risk.

As stated in the SNRA, the main threat to tax advisory and accountancy services, similar to the other professions involving the provision of legal advice, is infiltration or exploitation by organised crime. Professionals may be unintentionally involved in money laundering by these groups, but may also intentionally or negligently ignore the law in performing their due diligence obligations in respect of such clients.

According to the SNRA, organised crime groups often use tax advisors and accountants for advice and / or involve them in their money laundering systems. The services of tax advisors and accountants are considered useful in setting up money laundering systems because they are needed for certain types of activities and / or because access to specific tax expertise and skills can be helpful in money laundering. According to the SNRA, there is also evidence that some criminals seek to co-opt and knowingly involve tax advisors and accountants in their money laundering schemes. Professional tax advisors and accountants may be involved in the money laundering process to varying degrees. They may be consulted on how to circumvent and avoid certain legal frameworks, or they may be more proactive by directly supporting or coordinating the money laundering process.

Services provided by tax advisors and accountants are used for legitimate purposes. However, they can also support a variety of money laundering schemes.
However, the Chamber of Tax Advisors and Accountants in Austria has no indications that the professions are being exploited on a large scale for money laundering and terrorist financing activities. The criminal prosecutions and convictions reported to the Chamber on the basis of professional regulations show that only very occasionally are professionals proactively involved in money laundering schemes. Other statistics, such as searches of premises at the offices of tax advisors and accountants, also show that they are only rarely involved in money laundering and terrorist financing schemes.

Conclusion:
Based on the SNRA summary scenarios, which suggest a significant threat, the current national data show that, based on national data and statistics, there is no significant threat apparent in the tax consultancy and accountancy sector. In summary, the threat should be classified as moderately significant.

Vulnerability

Money laundering and terrorist financing:
As noted in the SNRA, the KSW would point out that the assessment of vulnerability to terrorist financing in connection with services provided by accountants and tax advisors was examined together with money laundering. Vulnerability to terrorist financing thus does not require a separate assessment.

In the SNRA summary scenarios, the vulnerability of services provided by tax advisors and accountants with regard to their exploitation for purposes of money laundering and terrorist financing was classified as significant. In the text which follows, we will analyse the national risk.

(a) Risk exposure:
Risks exist primarily as a result of the services offered by these professional groups.
Consequently, we will now provide an overview of the most relevant services of the two professional groups and their risk exposure:

Payroll accounting:
This service relates to the calculation of employees' salaries, the calculation of their claims for expense reimbursement, etc., up to and including the provision of support and representation to clients in payroll tax, social security and municipal tax audits. In the context of payroll accounting, the risk of these professional groups being exploited for purposes of money laundering and financing terrorism is considered lowly to moderately significant. Licenced professionals may identify and report illegal conduct, such as circumventing rules on undeclared employment, etc., in part, and with reference to Art. 77 para. 6 WTBG 2017.

Bookkeeping
The service area of bookkeeping includes, among other things, keeping clients' accounts on the basis of the documents provided by the client, preparing and submitting advance VAT returns, and providing monthly lists of balances for general ledger and subledger accounts. Here, too, the risk of the professions being exploited for money laundering and terrorist financing purposes is considered lowly to moderately significant. In this area of practice, licenced professionals can, under certain circumstances, identify anomalies and report any unlawful transactions. However, this can be made considerably more difficult by the

presentation of falsified receipts or turnover records. Here, again, we would refer to what is stated at the outset regarding Art. 77 para. 6 WTBG 2017.

Preparation of annual financial statements

The annual preparation of financial statements is one of the core activities for tax advisors and accountants. Licensed professionals are usually involved in all steps of the preparation of the annual financial statements. It is precisely this area of activity which illustrates the licensed professionals' indirect "observer role", already mentioned above. Although they are not directly involved in a company's financial and economic processes, in the course of preparing the annual financial statements they gain precise insights into a company's financial and economic processes. Tax advisors and accountants are thus able to identify suspicious circumstances with regard to money laundering and terrorist financing. In this regard, they have a reporting obligation to the Financial Intelligence Unit. Nevertheless, the risk of the professional groups being exploiting for money laundering and terrorist financing purposes when preparing annual financial statements is considered lowly to moderately significant. In this area of professional activity, only through a licensed professional's active involvement in untruthful preparation of annual financial statements is it likely that this could occur.

Consultancy (incl. tax return and expert opinions)

Consultancy activities are another focus of the services provided by tax advisors and accountants. These are primarily consultancy services in the area of tax law and accounting, but also consultancy services in connection with work-related issues, in matters of contributions, insurance and benefits of the social insurance institutions, as well as in the realm of corporate restructuring advice. In addition, other consultancy areas are mentioned in Art. 2 and 3 WTBG 2017, which these licensed professionals undertake in individual cases. In most of these consultancy areas, licensed professionals are also authorised to represent clients, such as in tax and criminal tax proceedings. In this context, they also prepare expert opinions on complex tax law issues.
Another major activity in this context is the preparation of regular tax returns for clients.

Here, too, similar arguments can be made to those given above regarding the preparation of annual financial statements. Here, too, the licensed professionals primarily assume an indirect "observer role". They are not directly involved in the financial and economic processes of the clients, but they may gain insight into their financial and economic affairs in the course of their work. Tax advisors and accountants are thus able to identify suspicious indicatations of money laundering and terrorist financing. In this respect, they have a duty to file an STR with the Financial Intelligence Unit of the Federal Ministry of the Interior. The risk of these professions being exploited for purposes of money laundering and terrorist financing is considered lowly to moderately significant.

Fiduciary activity (Treuhand)

In the course of their professional activities, tax advisors and accountants occasionally also act in a fiduciary capacity. This is usually a fiduciary activity in connection with the settlement of a transaction or holding of participations. Since these licensed professionals carry out financial transactions directly for their clients, their risk of being exploited for money laundering and terrorist financing purposes is considered moderately significant to significant. However, it should be pointed out that financial transactions carried out in this way are only carried out with the involvement of banks or financial institutions, which in turn are bound by the strict measures to prevent money laundering and terrorist financing. In this way, there are thus controls by the tax advisor/accountant on the one hand and by

the bank or financial institution on the other. Furthermore, tax advisors and accountants in Austria only perform fiduciary activities in isolated cases, such that this represents a rather insignificant practice area in relation to their other activities.

Audit services
In terms of audit services, both statutory and voluntary audits of financial statements as well as other statutory audits and other auditing assignments are carried out. The risk is again assumed to be lowly to moderately significant. Professionals who perform statutory audits of financial statements are audited as part of the regular quality assurance audits by the Auditor Oversight Authority (see below) and checked for their compliance with measures to prevent money laundering and terrorist financing.

Furthermore, the risk exposure can be determined by geographic risk and client risk.

Geographic risk
Tax advisors and accountants provide most of their services within Austria. Especially small firms of tax advisors and accountants, and firms in rural areas, usually only serve clients from their regional area. In contrast, there are large firms that are also active across borders. These are usually firms which are part of an international network (e.g. Big Four entities). Cross-border activities are primarily geared towards clients located 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 geographic distribution among the clients served:

- Around 85% domestic clients
- Around 10% clients from EU Member States
- around 5% clients from non-EU countries.

The geographical risk for services provided by tax advisors and accountants is therefore classified by the Chamber of Chartered Tax Advisors and Accountants as lowly to moderately significant. Where clients from high-risk countries are involved, the licensed professionals are obliged to apply increased due diligence measures in connection with the measures to prevent money laundering and financing of terrorism; see remarks on the risk-mitigating measures.

Client risk
As noted earlier, tax advisors and accountants act for a wide range of clients. These may range from individuals and one-man companies to large and complex companies and networks. Furthermore, licensed professionals sometimes also work for institutions under public law as well as municipalities and churches.
The economic sectors of the clients are thus also broadly diverse. They include (financial) service companies, operating companies as well as construction companies and the like.

For this reason, we must assume that the risk in the area of clientele is moderately significant. A concrete determination of the money laundering and terrorist financing risk of a client usually requires a case-by-case assessment by the tax advisor/accountant as part of the obligatory risk assessment.

However, an increased risk is indicated for certain clients.
This will, for example, be the case if the client is a PEP or a family member of a PEP or a person close to the PEP.

Certain industries may also suggest a potentially increased risk. These include, in particular, industries which use cash to a particularly large extent (e.g. restaurants, hotels, brothels, gambling establishments, etc.), companies in the construction industry and property developers, as well as real estate trade and trade in high-value goods (e.g. precious metals, gems, jewellery, watches, objects of art, antiques, motor vehicles, ships, motorboats, aircraft, machinery, etc.) and import/export companies.

However, there are also circumstances which indicate a low risk of money laundering and terrorism on the part of the client.

This holds true above all in respect of public listed companies that are subject to disclosure obligations that impose requirements to ensure adequate transparency with regard to beneficial owners. Furthermore, a low risk is similarly indicated for public administration and public institutions and companies.

(b) Risk awareness:
Tax advisors and accountants must always apply strict legal (professional) standards of care and observe general professional ethics rules when providing their services.

Services in the areas of tax consultancy and accountancy are also mostly geared towards longer-term business relationships. This also creates a certain relationship of trust between the professionals and their clients. Tax advisors and accountants can thus evaluate the economic and financial affairs of their clients well and identify possible risks. Occasionally, however, they also do shorter and one-off jobs, especially in the area of consultancy services.

Furthermore, they are obliged by law to keep their professional knowledge up to date at all times in accordance with Art. 71 para. 3 WTBG 2017. The Chamber of Tax Advisors and Accountants is always keen to train its members in respect of money laundering and terrorist financing and to keep them informed. The Chamber of Tax Advisors and Accountants does this by organising information events and themed evenings and by sending out newsletters. In addition, licensed professionals can obtain information on the prevention of money laundering and terrorist financing from the Chamber of Tax Advisors and Accountants in writing and by telephone. All of this raises risk awareness in the profession.

The Chamber of Tax Advisors and Accountants also regularly submits requests for information and intelligence to relevant authorities, such as the FIU, in order to obtain the latest intelligence in the areas of money laundering and terrorist financing. These findings are then shared with the professional groups.

Finally, licensed professionals are obliged to train their employees regularly on the topics of money laundering and terrorist financing. These training sessions must be documented and are also audited by the Chamber of Tax Advisors and Accountants.
Thanks to these measures, one may say that there is broad risk awareness in the profession with regard to money laundering and terrorist financing.

(c) Legal framework and supervision/governance:
In performing their professional work, tax advisors and accountants must always comply with the professional regulations and measures for preventing money laundering and terrorist financing, which are set out in Art. 87 - 105 WTBG 2017. In addition to these legal

provisions, licensed professionals are also subject to the Ordinance of the Chamber of Tax Advisors and Accountants on the Directive on the Prevention of Money Laundering in the Exercise of the Accounting Professions (KSW-GWPRL 2017), which prescribes further measures, orders and specifications.
Pursuant to Art. 101 WTBG 2017, it is the responsibility of the Chamber of Tax Advisors and Accountants, as the representative professional body, to supervise compliance with the measures for the prevention of money laundering and terrorist financing. For this purpose, 1.5 full-time employees are employed in the Chamber office itself, who are supported by the Committee for Supervision of Money Laundering Prevention, consisting of 8 members of staff, and the 21 experts who carry out on-site inspections.

Supervisory audits of the Chamber of Tax Advisors and Accountants pursuant to Art. 102 WTBG 2017
The Chamber of Tax Advisors and Accountants conducts regular supervisory audits of its members to oversee compliance with measures to prevent money laundering and terrorist financing. These audits are carried out as general audits which are not based on specific cases and on the basis of a risk-based approach. In addition, the Chamber of Tax Advisors and Accountants may, of course, also carry out an *ad hoc* audit based on a specific case.

As already mentioned, the audits which are not based on a specific case are carried out on the basis of a risk-based approach. The specific professionals to be audited are selected on a random basis. The audits can be carried out in two different ways.

Audits may, firstly, be done in the form of an off-site examination, in which the evaluation is carried out on the basis of internal documents and information provided by the licensed professional. Secondly, they may be done in the form of an inspection at the business of the licensed professional, which may include a random inspection of their mandate files. Such inspections must be carried out by experts within the meaning of Art. 103 WTBG 2017. Such experts come from the profession of tax advisors and accountants and are selected from the group of investigation commissioners pursuant to Art. 140 WTBG 2017 or quality auditors pursuant to Art. 26 para. 5 Supervision of Auditors Act [*APAG*]. An additional requirement is proof of relevant training in the field of prevention of money laundering and terrorist financing.

Audits as part of a quality assurance audit
Licensed professionals who are entered on the public register pursuant to Art. 52 APAG are exempt from the above-referenced general audits by the Chamber of Tax Advisors and Accountants. However, these authorised professionals are audited by the Auditor Appointment Authority (*APAB*) as part of their regular quality assurance audits. In order to ensure uniformity of procedure for the ad hoc audits of the Chamber of Tax Advisors and Accountants and the *APAB*, the Chamber of Tax Advisors and Accountants has drawn up a communique on the procedure for the audits. Should problematic findings be made by the *APAB*, the *APAB* is also obliged to notify the Chamber of Tax Advisors and Accountants, as the Chamber of Tax Advisors and Accountants remains the sole supervisory authority for the prevention of money laundering and terrorist financing. Furthermore, it is also open to the Chamber of Tax Advisors and Accountants to conduct an *ad hoc* audit of the licensed professional, for instance if there are grounds for suspicion.

Conclusion:
Based on the SNRA summary scenarios, which suggest significant vulnerability, the framework conditions presented lead us to classify the vulnerability of tax advisors and

accountants to abuse for the purposes of money laundering and terrorist financing as moderately significant.

Risk-mitigating measures

The risk-mitigating measures of tax advisors and accountants are set out in Art. 89 - 100 WTBG 2017.
In the text below, we list due diligence obligations applicable to tax advisors and accountants.

Identification of the client
Where the client is a natural person, identification must be performed by means of a current official photo ID. The same applies to the legal representatives of legal entities as clients, and if agency power is only granted collectively, then each member of the group with agency power must be identified (Art. 90 para. 1 WTBG 2017). If no current official photo ID is available for the identification of a natural person, Art. 1 para. 1 Directive on the Prevention of Money Laundering in the Exercise of the Accountancy Professions [KSW-GWPRL] stipulates that the verification may also be based on other sources, taking a risk-based approach. In this context, information from reliable sources is considered credible. These include courts and other state authorities, tax advisors, accountants and persons with comparable foreign professional authorisation, notaries, lawyers and credit institutions, provided they do not have their official practice, registered office or domicile in a non-cooperating state within the meaning of Art. 94 para. 5 WTBG 2017.

If the client is a legal entity, licensed professionals must establish the identity of the persons authorised to represent the client (where agency power is exercised only collectively, then the identity of each member of the group authorised to represent the client must be established) and, as a rule, must verify their identity by checking their identification. The identity of beneficial owners must be established, e.g. by questioning the client's legal representatives. Status as beneficial owner as well as the identity of beneficial owners must be verified by taking risk-oriented and appropriate measures, e.g. by inspecting the commercial register or the Register of Beneficial Owners (WiEReG). Identification of the client includes a duty of tax advisors and accountants to take reasonable measures to understand the ownership and control structure of the client. If in an individual case there is only a low potential risk that the services of the licensed professional will be exploited for money laundering or terrorist financing purposes, it may be sufficient, if there is also no other indication of increased risk, to use general means to obtain a general understanding of the ownership and control structure of the client.

In the case of other representatives, the identify of the client as well as the representative must be checked and both the identity of the representative and the valid power of attorney must be verified. Section 1 para. 3 KSW-GWPRL requires a written power of attorney to be obtained; only in the case of professional party representatives is it sufficient to refer to a granted power of attorney together with proof of a professional licence.

PEP query
When entering into a new business relationship, tax advisors and accountants must determine whether their client is a PEP. Section 94 para. 1 subpara. 4 WTBG 2017 (enhanced due diligence) makes clear that PEPs, their family members and persons known to be related to them are to be treated equally from a risk perspective. This group of persons is defined in Art. 87 para. 2 subparas. 14-16 WTBG 2017. It is the responsibility of the professional to

determine how to check whether a principal or a beneficial owner belongs to this group of persons. For the most part, this is done by querying specialised databases to perform relevant checks on persons, especially with regard to their classification as politically exposed persons (PEP).

Firm risk assessment
The licensed professional must classify all activities typical for the profession which are offered or carried out by his or her firm within one of the risk categories high/medium/low, according to the risk of exploitation for money laundering or terrorist financing purposes on the basis of the EU risk assessments, the National Risk Assessment as well as the risk factors of Annexes 1 - 3 of the 4th Anti-Money Laundering Directive.

Policy Manual for Tax Consultancy and Accountancy Firms
Pursuant to Art. 88 para. 3 WTBG, the licensed professional must summarise all strategies and methods used to fulfil anti-ML obligations, as well as the internal documents and working papers used for this purpose and the documentation systems used in a Policy Manual for the accountacy firm. All members of staff must be made aware of this Policy Manual and this must be documented.

In this context, the size and complexity of the firm, the duration and type of services rendered, the identity of a client or a beneficial owner, the structure of the client and the regions in which the licensed professional renders his services are taken into account. The firm's guidelines must also contain information on the Chamber of Tax Advisors and Accountants whistleblower system and, depending on the size of the firm, on the firm's internal whistleblower system. It must also indicate the place where the currently applicable firm whistleblower guide can be viewed by employees, as well as clarifications as to who is responsible for answering questions about it. In addition, reference should be made to the right of inspection of the Chamber of Tax Advisors and Accountants or, if applicable, of the audit supervisory authority with regard to anti-ML audits.

Money Laundering Officer
Licensed professionals shall designate a special officer for money laundering and terrorist financing issues if this is necessary in light of the type and scope of their business activity (Art. 99 para. 2 WTBG 2017). The licensed professional must ensure that the money laundering officer has sufficient professional qualification, knowledge and experience at all times (professional qualification) and is a person of integrity (personal reliability).

AML documentation
Decisions on the substance of mandate-specific due diligence obligations and their basis must be documented in a risk-based manner. Art. 98 WTBG (documentation and record-keeping obligations) stipulates that licensed professionals are generally obliged to store

1. documents which are required to fulfil due diligence obligations towards clients,
2. supporting documents and records of transactions,
3. documents relating to suspicious transaction reports submitted and
4. documents related to the risk class of the client

for five years from the date of the last transaction (or from the execution of the relevant transaction). The period runs from the end of the calendar year to which the last transaction relates.

Rules relating to staff
Pursuant to Art. 99 para. 1 subpara 2 WTBG, licensed professionals must fulfil special duties with regard to their staff:
Pursuant to Art. 99 para. 1 subpara 2 letter a WTBG 2017, staff must be screened for money laundering or terrorist financing at the time of recruitment. Pursuant to Art. 99 para. 1 subpara 2 no. b and c WTBG 2017, employees must be demonstrably familiarised with the firm's internal rules and trained in special training programmes. The completion of the training measure as well as the training content must be documented in any case.

Risk profile
A risk profile must be prepared for each mandate in order to assess the risk of money laundering or terrorist financing. For each mandate, the licensed professional must prepare a risk profile on the basis of all information received about the client, the service and the tax consultancy / accountancy firm risk and related information and keep it up to date for the duration of the business relationship. With regard to the service risk, the evaluation in the firm's risk assessment shall be used.
The level of the mandate-specific risk which is noted in the risk profile also determines whether reduced due diligence obligations or enhanced due diligence obligations should apply. The frequency of the regular updating of the documented data also depends on this risk classification. In this context, data relating to a mandate with an increased risk must be updated more frequently than data relating to a mandate with a lower risk, even if there is no specific reason for doing so. In the case of mandates with increased risk, at least an annual update of the risk profile will be necessary.

Due diligence in the customer onboarding process
In the case of a natural person as principal, identification must be undertaken by means of a current official photo ID. The same applies to groups of legal representatives where agency authority is exercised only by a group, in which case each member of the group authorised to represent the client must be identified (Art. 90 para. 1 WTBG 2017 - scope of due diligence). A photo ID that expires in the course of the business relationship does not change the original identification. Suitable photo IDs must be provided with a non-interchangeable recognisable head picture of the person to be identified (i.e. a photo which has been affixed by the authority) and which does not obviously differ from the person identifying himself/herself personally.
If no current official photo ID is available for identification of a natural person, Art. 1 para. 1 KSW-GPRL (specific form of due diligence obligations) stipulates that the verification may also be based on other sources, taking a risk based approach. In this context, information from reliable sources is considered credible. These include courts and other state authorities, tax advisors, accountants and persons with comparable foreign professional licences, notaries, lawyers and credit institutions, unless they have their official area of activity, registered office or domcile in a non-cooperating state within the meaning of Art. 94 para. 5 WTBG (Enhanced Due Diligence).

Audits of unusual transactions
Unusual transactions within the meaning of Art. 94 para. 1 subpara. 1 WTBG 2017 will in any event require licensed professionals to set the risk class to high, pending investigation. They must also be examined to determine whether the origin and use of funds is legal. This must be done by appropriate means. An uninvestigated factual situation could expose the licensed professional firstly to the risk of abetting criminal money laundering within the meaning of Art. 165 StGB, and secondly to the risk of a violation of his or her duty to submit

a suspicious transaction report on the presence of funds from criminal acts pursuant to Art. 96 WTBG 2017.

Suspicious cases

To trigger a duty on the part of a tax advisor or accountant to submit a report, it is sufficient that there is a suspicion that financial resources within the meaning of Art. 87 para. 2 subpara. 6 WTBG 2017 originate from criminal activities within the meaning of Art. 87 para. 2 subpara. 2 WTBG 2017 or are connected with terrorist financing, irrespective of the respective amount. Licensed professionals must carry out a more detailed examination of the available indications in the event of suspicious circumstances. Section 87 para. 2 subpara. 7 WTBG 2017 defines reasonable suspicion as "the assumption of the likelihood of the existence of a certain circumstance based on knowledge of sufficient factual indications. This assumption must go beyond a mere presumption." Pursuant to this definition, a suspicion exists when "sufficient factual indications justify the assumption of the likelihood of the existence of certain circumstances; a suspicion is more than a mere presumption. Suspicion can only ever arise on the basis of inferences from facts - knowledge of facts can be used to infer the existence of an offence according to life experience." Finally, it should be noted that to the extent one assumes that the requirements for "justified grounds of suspicion" are lower than those for suspicion, doubts will be indicated, because it is difficult to see in what way suspicion – in view of the definition presented – would set higher requirements than the existence of justified grounds for suspicion of contact with incriminated assets. (Brandl/Bülte, *Die Geldwäsche-Verdachtsmeldepflicht und das Vertrauensverhältnis zwischen Berater und Mandant in Leitner/Brandl* (eds.), Finanzstrafrecht 2019)

Reporting obligation

If the licensed professional suspects in the course of his or her professional activities that financial resources, regardless of the respective amount, originate from criminal activities or are connected to terrorist financing, he or she must inform the Financial Intelligence Unit without delay on his or her own initiative by means of an STR (Art. 96 para. 1 WTBG 2017). Furthermore, he/she must consider filing an STR if he is unable to fulfil his/her due diligence obligations with regard to a client in terms of establishing and verifying the identity of the client or the beneficial owner or assessing and obtaining adequate information about the purpose and intended nature of the business relationship (Art. 96 para. 3 WTBG 2017).

In addition, pursuant to Art. 96 para. 2 WTBG 2017, he/she must immediately, directly or indirectly, provide the Financial Intelligence Unit with all additional information upon written request, provided that this does not conflict with prohibitions under procedural or professional law or with a party's right to refuse to testify. The reporting obligation as well as the general application of the provisions on money laundering prevention in Art. 88 - 100 WTBG 2017 should be understood as referring exclusively to facts that occurred during the exercise of the professional activity of the licensed professional.

Measures taken by the Chamber of Tax Advisors and Accountants to minimise risk

In addition to the following risk-mitigating measures, we also refer to the explanations under the item "(c) Legal framework and supervision/governance", which also qualify as risk-mitigation measures of the Chamber of Tax Advisors and Accountants.

Training by the Chamber of Tax Advisors and Accountants in the area of prevention of money laundering and terrorist financing

The Chamber of Tax Advisors and Accountants always takes efforts to train its members in the area of money laundering and terrorist financing and to keep them informed. The Chamber of Tax Advisors and Accountants does this by organising information events and themed evenings and by sending out newsletters. In addition, licensed professionals can also obtain information from the Chamber of Tax Advisors and Accountants in writing and by telephone with regard to the prevention of money laundering and terrorist financing. Furthermore, tax advisors and accountants are required by law to provide evidence of a specified level of continuing education. These further training courses are mostly completed at the Academy of Tax Consultants and Auditors (*ASW*), a 100% subsidiary of the Chamber of Tax Advisors and Accountants. In recent years, the ASW has greatly expanded its range of teaching and training courses with a focus on the prevention of money laundering and terrorist financing. The ASW also functions as the training academy for trainees. Thus, as part of their professional traning, trainees are increasingly trained on the prevention of money laundering and terrorist financing. The ASW's money laundering prevention training app also deserves mention here. The training app is used by many licensed professionals for further training and for training law firm employees and helps to raise awareness of members of the profession as well as their employees.

The Chamber of Tax Advisors and Accountants whistleblower system pursuant to Art. 100 WTBG 2017

KSW has had a whistleblower system in place since 1 January 2019. The whistleblower system is accessible to everyone and facilitates anonymous reporting of licensed professionals who fail to comply with the measures for the prevention of money laundering and terrorist financing specified in WTBG 2017. Each report by a whistleblower is examined by the Chamber of Tax Advisors and Accountants and may, if necessary, lead to the initiation of a case-specific audit and of disciplinary proceedings.

Prior to May 2020, only one report was filed via the Chamber of Tax Advisors and Accountants whistleblower system. However, that report concerned the alleged money laundering activity of a client of a licensed professional, which is why it was forwarded to the Financial Intelligence Unit.

Overall risk

The overall risk of the tax consultancy and accountancy sectors is classified as lowly to moderately significant.

Recommendations

In order to improve the prevention of money laundering and terrorist financing, the Chamber of Tax Advisors and Accountants would encourage better and more extensive exchange of information between authorities. For example, the Financial Intelligence Unit should actively forward information to the Chamber of Tax Advisors and Accountants if it relates to licensed professionals or if cases are discovered that indicate an increase in the exploitation of the services of tax advisors and accountants. Furthermore, the exchange of information with other authorities and institutions, such as the FMA, the OENB or financial institutions, should be intensified and encouraged further.

Sector risk assessment - Accountancy

Services of certified management accountants, accountants and payroll accountants

General information

From the date of entry into force of the Federal Act on the Accountancy Professions (Accountancy Act 2014 - **BiBuG 2014**; Federal Law Gazette I No. 191/2013), as from 1 January 2014, the **President of the Austrian Federal Economic Chamber [*WKÖ*] has been responsible for the accountancy professions as the Authority for the Accountancy Professions**, i.e. **as a federal authority acting within the remit delegated by the Federal Ministry of Digital and Economic Affairs**. Responsibility for the **operational exercise** of this authority is vested in the **Office of the Authority for the Accountancy Professions** at the Austrian Federal Economic Chamber.

Pursuant to Art. 1 BiBuG 2014, the accounting professions are **certified management accountants, accountants and payroll accountants.**

Pursuant to Art. 6 BiBuG 2014, only **natural persons who have been publicly appointed** and **companies that** have been **licensed** may exercise the powers within the respective scope of authorisation pursuant to Art. 2-5 BiBuG 2014.

Licensed professionals in the accounting profession are obliged to implement the **measures for the prevention of money laundering and terrorist financing pursuant to Art. 43-52d BiBuG 2014.**

Pursuant to Art. 52f BiBuG 2014, the President of the WKÖ is responsible for **supervising compliance with these provisions**.

Threat

Terrorist financing:
In the SNRA summary scenarios, the **threat of professional accountants** being abused for terrorist activities was classified as **significant**. In the text which follows, we will analyse the **national risk.**

The picture of the accounting professions sector is **completely clear** from a terrorist financing perspective: accounting **professionals do not** come into **contact with TF-related risks.**

This picture emerges very clearly **from the current information (survey of 4213 licensed professionals, version of: 31 July 2020)** available to the Authority for the Accountancy Professions, based on its performance of its supervisory duties pursuant to Art. 52f BiBuG 2014.
This is probably primarily due to the **typical client structure** and the **services typically provided** by the accountancy professions.

The average professional in the accountancy professions does **not** have **any conspicuous clients** from the perspective of terrorist financing and is **completely familiar with his clients'**

business conduct. This is due *inter alia* to the fact that clientele of these licensed professionals are located **almost exclusively in the accountancy professional's local environment and the accountant has known his or her clients for a significant time**.

This information is further confirmed by the **absence to date (as of 25 February 2021)** of any report via the **internet-based whistleblowing system of the Authority for the Accountancy Professions** pursuant to Art. 52e BiBuG 2014.

The BMDW and the Financial Intelligence Unit, as part of their duties under **Art. 52i para. 2 BiBuG 2014,** have informally provided information to the Authority for the Accountancy Professions.

Conclusion:
Based on the SNRA summary scenarios, which suggest a significant threat, the current national data show the opposite for the reasons given above. In summary, the threat for the accountancy professions should be classified as lowly significant.

Money laundering:
In the SNRA summary scenarios, the **threat of accountancy professionals** being abused for money laundering was classified as **significant.** In the text which follows, we will analyse the **national risk.**

The picture of the accountancy professions sector is **completely clear** from a terrorist financing perspective: **accounting professionals rarely** come into **contact with ML-related threats.**
This picture emerges in a similarly clear manner **from the current information (survey of 4213 licensed professionals, date: 31 July 2020)** available to the Authority for the Accountancy Professions, based on its performance of its supervisory duties pursuant to Art. 52f BiBuG 2014.
Furthermore, this picture **also applies** - with very slight fluctuations - to the **individual federal provinces**.

Due to the **tendency of these licensed professionals to be organised within small business structures** (with 1.4 employees on average), they seem to have a **fundamental reluctance to accept individual clients with a potentially high ML risk,** or **are very cautious in accepting them,** fearing the administrative burden and/or sanctions/consequences associated with such clients. The **typical client structure** - already referred to above - consisting of clients who **come almost exclusively from the local business environment and have been known to the accountancy professionals for a longer time should** also be mentioned in this context.

The **geographical nature of the clientele of the accountancy professions** is **clear** from the current information (as of 31 July 2020) available to the Authority for the Accountancy Professions based on its performance of its supervisory duties under Art. 52f BiBuG 2014. The clients of the accountacy professions are:

- **97.79% Austrian clients** with their exclusive main residence in Austria
- **2.08% clients from the EU**
    - clear link to the CEE region or neighbouring Member States
    - strongest links to Germany
- **99.87% clients from low-risk countries**
- **0.13% clients from high-risk countries**
    - clear links to the CEE region: especially Serbia, Bosnia and Turkey

- fairly relevant links to China and Russia

This information is, in turn, confirmed by the **absence to date (as of 25 Febuary 2021)** of any report via the **internet-based whistleblowing system of the Authority for the Accountancy Professions** pursuant to Art. 52e BiBuG 2014.

The BMDW and the Financial Intelligence Unit, as part of their duties under Art. **52i para. 2 BiBuG 2014,** have informally provided information to the Authority for the Accountancy Professions.

Conclusion:
Based on the SNRA summary scenarios, which suggest a significant threat, the current national data show the opposite for the reasons given above. In summary, the risk for the accountancy professions should be classified as lowly significant.

Vulnerability

Terrorist financing:
In the SNRA summary scenarios, the **vulnerability of licensed professionals from the accounting professions** with regard to abuse for purposes of terrorist financing was classified as significant. In the text which follows, we will assess the **national vulnerability.**

(a) Risk exposure:
As described above, the picture of the accountancy professions sector from a terrorist financing perspective is **completely clear**: **licensed professionals** from the accountancy professions **do not** come into **contact with TF-related risks**.
The accountancy professions sector does **not seem to be attractive to TF** as a general rule **due to the services typically provided by these professionals.**

(b) Risk awareness:
There is a **high level of risk awareness** among all professionals in the accountancy professions.

(c) Legal framework and supervision/governance:
Licensed professionals from the accountancy professions are **obliged to implement** the **measures for the prevention of money laundering and terrorist financing pursuant to Art. 43-52d BiBuG 2014 and to comply with their obligations** in this respect.
Violations of the professional **obligations in relation to the prevention of ML/TF are punishable under Art. 52j-52k BiBuG.**

The Authority for the Accountancy Professions, which is responsible for the supervision of compliance with the precautionary measures for prevention of ML/TF, has prepared a **standardised risk assessment** (with elaborations and definitions) for its survey of licensed professionals which has been carried out last year (see the website of the Authority for the Accountancy Professions at https://www.wko.at/site/bilanzbuchhaltung/verhinderung-geldwaesche-terrorismusfinanzierung.html). That risk assessment is intended to support these licensed professionals in fulfilling their professional obligations with regard to the prevention of ML/TF and can also be used by the Authority as a **basis for a specific case-related or general audit** pursuant to Art. 52g *et seq.* BiBuG.

Human and financial resources:
The Authority for the Accountancy Professions has one **part-time employee available to deal with** the area of ML/TF prevention.

Conclusion:
Based on the SNRA summary scenarios, which suggest a significant level of vulnerability, the framework conditions presented here mean that the vulnerability of the accountancy professions to exploitation for the purposes of terrorist financing should be classified as lowly significant.

Money laundering:
In the SNRA summary scenarios, the **vulnerability of licensed professionals from the accounting professions** with regard to exploitation for purposes of money laundering was classified as **significant**. In the text which follows, we will analyse the **national vulnerability.**

(a) Risk exposure:
As described above, the picture of the accountancy professions from a money laundering perspective is **very clear**: **licensed professionals** from the accountancy professions **only rarely come into contact with ML-related risks**.

Vulnerability **from a geographical point of view** is **extremely negligible**: Due to the fact that the typical client structure consists almost exclusively of Austrian or geographically low-risk clients from the immediate vicinity, there is an **increased sensitivity regarding clients who do not fall into this typical pattern.**

Vulnerability **in terms of activities relating to the products, services, transactions and/or distribution channels offered by clients is** also **negligible**.

By contrast, vulnerability **in terms of of the activities of the clients** does exist to **a small, albeit relevant extent** with regard to **transactional activities of clients who use cash to a large extent**. This aspect is partly **due** to the **client structure of** the accountancy professions, which is largely made up of catering, trade and crafts.

This picture also **applies** - with very slight fluctuations - to the **individual federal provinces**. Conclusion: Lowly significant risk, for the reasons given.

(b) Risk awareness:
There is a **high level of risk awareness** among all licensed professionals in the accountancy professions.

(c) Legal framework and supervision/governance:
Licensed professionals from the accountancy professions are **obliged to implement** the **measures for the prevention of money laundering and terrorist financing pursuant to Art. 43-52d BiBuG 2014 and to comply with their obligations** in this respect.
Violations of the professional **obligations in relation to the prevention of ML/TF are punishable under Art. 52j-52k BiBuG.**

The Authority for the Accountancy Professions, which is responsible for the supervision of compliance with the precautionary measures for prevention of ML/TF, has prepared a **standardised risk assessment** (with elaborations and definitions) for its survey of licensed professionals which has been carried out last year (see the website of the Authority for the Accountancy Professions at https://www.wko.at/site/bilanzbuchhaltung/verhinderung-

geldwaesche-terrorismusfinanzierung.html). That risk assessment is intended to support these licensed professionals in fulfilling their professional obligations with regard to the prevention of ML/TF and can also be used by the Authority as a **basis for a specific case-related or general audit** pursuant to Art. 52g *et seq.* BiBuG.

Human and financial resources:
The Authority for the Accountancy Professions has one **part-time employee available to deal with** the area of ML/TF prevention.

Conclusion:
Based on the SNRA summary scenarios, which suggest a significant level of vulnerability, the framework conditions presented here lead us to class the vulnerability of licensed professionals from the accountancy professions to abuse for the purposes of money laundering as lowly significant.

Risk-mitigating measures

- Continual raising of awareness in the context of the duty to provide further training pursuant to Art. 33 para. 3 BiBuG 2014
- Raising awareness in the context of the implementation of the supervisory duties pursuant to Art. 52f BiBuG 2014 by the Authority for the Accountancy Professions, for example by providing case studies and guidance on its website (https://www.wko.at/site/bilanzbuchhaltung/verhinderung-geldwaesche-terrorismusfinanzierung.html)

Overall risk

In summary, the risk should be classified as lowly significant.

Sector risk assessment – Gambling services providers

Casino gambling (Casinos)

General information

Casino gambling constitutes gambling services within the meaning of Directive (EU) 2015/849 (Art. 3 para. 14), which are offered in the form of terrestrial gambling (at a physical location, automated or in the form of live play). Currently, 12 casinos are operated by a single provider within the federal territory of Austria.

Threat

Terrorist financing:
Based on the SNRA summary scenarios, the threat of casinos being abused for terrorist activities was classified as not relevant. The national risk is also classified as not relevant.

Conclusion:
In summary, the threat should be classified as not relevant.

Money laundering:
Based on the SNRA summary scenarios, the threat was classified as **very significant**. In the text which follows, we will analyse the national risk. Threats exist due to unknown customer origin, multiple registrations of a single person, use of cash, use of foreign currencies, multiple use of payment methods by multiple customers, gambling by politically exposed persons (PEP), gambling by persons listed on sanction lists, exploitation of portfolio accounts, circumvention of deposit limits, malversations by an employee (issuing of winnings confirmations/collusion of guest and dealer), conversion of cash, counterfeit money, collusion of customers/guests, failure to follow up on a suspicion of money laundering. Overall, the risk of these threats should be classified as **significant.**

Conclusion:
Based on the SNRA summary scenarios, which suggest a very significant level of threat, the current national data show a significant threat. In summary, the risk should be classified as significant.

Vulnerability

Terrorist financing:
In the SNRA summary scenarios, the vulnerability of casinos to exploitation for the purposes of terrorist financing was classified as **not relevant.** National vulnerability is also assessed as **not relevant.**

Conclusion:
In summary, the vulnerability of casinos to exploitation for the purposes of terrorist financing should be classified as not relevant.

Money laundering:
In the SNRA summary scenarios, the vulnerability of casinos to explitation for the purposes of money laundering was classified as **moderately significant.** In the text which follows, we will analyse the national vulnerability:

(a) Risk exposure:
There is a very high proportion of cash revenues and the possibility of converting cash into play money and vice versa.

(b) Risk awareness:
Not least due to the requirements of the AMLD, enhanced due diligence obligations have been included in the national gambling legislation. Admission to casinos is only permitted upon presentation of an official photo ID. Participation in games is predominantly 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 regular participation of employees in money laundering prevention training.

(c) Legal framework and supervision/governance:
Art. 31c of the Games of Chance Act [GSpG] in connection with the FM-GwG provides for comprehensive due diligence obligations for the operators of casinos (according to the respective situation, in addition to the determination of the identity of the visitors, in particular the determination of the origin of the funds or the beneficial owner).

Conclusion:
Based on the SNRA, which suggests moderately significant vulnerability, the framework conditions we have presented lead us to class the vulnerability of casinos to abuse for money laundering purposes as moderately significant.

Risk-mitigating measures

Pursuant to Art. 31c *GSpG* in conjunction with the FM-GWG, comprehensive due diligence obligations with regard to the prevention of money laundering include (in addition to the duty to prepare a risk assessment and the complete identification of visitors) the identification of a trustor/beneficial owner and of the origin of funds and the verification of the purpose/type of business relationship as well as continuous monitoring of the same and the provision of the documentation required by the Games of Chance Act. The Games of Chance Act obliges the Federal Minister of Finance to provide casino operators with up-to-date information on methods of or criteria for identifying money laundering and terrorist financing. The Federal Minister of Finance is also required to ensure timely feedback regarding suspicious transaction reports for money laundering or terrorist financing and the measures taken in response, and to set up a whistleblower system for reporting violations of anti-ML regulations.

Overall risk

In summary, the risk should be classified as **moderately significant.**

Recommendations

Further intensify cooperation between companies and authorities and provide information as promptly as possible in cases of suspected money laundering.

Classic lotteries, other electronic lotteries, 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 locations) and **other electronic lotteries** (direct participation in the game of chance by the player via electronic media and a centrally initiated decision on the outcome of the game, e.g. **online gaming**). Currently, all forms of lotteries are operated by a single provider.

Threat

Terrorist financing:
Both the SupraNational Risk Assessment and the National Risk Assessment reach the conclusion that the threat of lotteries being exploited for terrorist activities should **not** be classified as **relevant.**

Conclusion:
In summary, the risk should be classified as not relevant.

Money laundering:
In the SNRA summary scenarios, the threat with regard to **electronic lotteries via VLT** was classified as **moderately significant** and with regard to **other electronic lotteries** it was classified as **significant.** In the text which follows, we will analyse the national risk.

- With regard to classic lotteries, no national threats can be identified. The sale of classic lottery products (especially lottery tickets, instant lotteries) takes place exclusively via sales affiliates in Austria and sales are transacted in euros. Any winnings are determined in the course of a public drawing supervised by a notary or, in the case of instant lotteries, are already determined in advance and thus also exclude the possibility of malversation by employees. Due to the anonymity of the winners, contact by criminals with the intention of acquiring and cashing in a winning ticket for money laundering purposes is also very unlikely. Moreover, winners with prize payouts of EUR 1,000.10 or more are identified. The national risk of classic lotteries can thus be classified as low.
- National threats in the realm of electronic lotteries via video lottery terminals (VLT): The threats of a lack of face-to-face identification, of multiple registration of a person, multiple use of the means of payment by multiple customers, marked money and counterfeit money are mitigated in that players have to register and identify themselves with an official photo ID before participating in the game. Moreover, participation in the game is only possible by means of a personalised player card, thus excluding the possibility that a person can register multiple times. When changing cash for play money, the banknotes are checked by a banknote acceptor in order to exclude the possibility that marked money or counterfeit money might be introduced. Non-cash payments are only processed by an employee who checks the identity of the customer, which is why it is also not possible for the same non-cash means of payment to be used by multiple customers. The national risk is therefore classified as low.
- National threats in the area of other electronic lotteries are: No face-to-face identification, multiple registrations by a single person, multiple use of the means of payment by multiple customers, exploitation of custodial accounts, circumvention of deposit limits, participation in games by politically exposed persons (PEP), participation in games by persons listed on sanction lists, collusion of

customers in poker games and the failure to deal with suspicions of money laundering. At the national level, a moderately significant risk can therefore be assumed.

Conclusion:
Based on the SNRA summary scenarios, which suggest a moderately significant threat, the current national data reveal a lowly significant risk overall. In summary, the risk should be classified as lowly significant.

Vulnerability

Terrorist financing:
Based on the SNRA summary scenarios, the vulnerability of lotteries with regard to exploitation for purposes of terrorist financing was classified as **not relevant**. The national vulnerability should also be assessed as **not relevant.**

Conclusion:
In summary, one can assume that that there is no relevant vulnerability present.

Money laundering:
In the SNRA summarised scenarios, vulnerability with regard to exploitation for purposes of money laundering was classified as **moderately significant** for classic lotteries, **moderately significant** for electronic lotteries via video lottery terminals (VLT) and **significant** for other electronic lotteries. In the text which follows, we will analyse the national vulnerability:

(a) Risk exposure:
With regard to **classic lotteries,** there is a risk of money laundering in that a winning ticket is acquired from the winner and subsequently redeemed. With regard to **electronic lotteries via VLT,** there is a risk due to cash turnover or the changing of cash into play money and back via player cards. **Other electronic lotteries** pose the risk that players will take part in the game of chance under a false identity due to lack of face-to-face identification as well as the risk of the lack of knowledge of the origin of funds due to the possibility of paying for their stakes by means of Paysafe cards and Euro vouchers.

(b) Risk awareness:
The risk of third parties acquiring and redeeming a winning ticket in **classic lotteries** is countered by the fact that winners are anonymous. This makes it virtually impossible for criminals to contact the winner in order to acquire the winning ticket from him or her and then redeem it themselves. In addition, identification is mandatory for payouts of EUR 1,000.10 or more. In the case of **electronic lotteries via VLT,** stake limits and enhanced due diligence obligations apply when changing amounts of EUR 2,000 or more into play money and vice versa. Moreover, participation in electronic lotteries via VLT with a personalised player card is only possible where the lottery player produces an official photo ID. With regard to **other electronic lotteries,** there are stricter requirements for registration: Participation in the lottery is only possible after personal data has been recorded. The data are verified via Deltavista and are also checked against the central population register. In addition, stakes are limited to a maximum of EUR 800 per registered player and week for all payment methods. Withdrawals from the player's electronic gaming balance are made by transfer to the player's bank account held in the EEA region, which he has previously disclosed to the lottery operator. The account details must be disclosed when the first request for a payout is made. If the player has not yet undergone extended identification by this time, he or she must undergo this immediately before making the first payout request. Pursuant to Art. 6 para. 4 FM-GwG, the following identification procedures are available for

this purpose: Online verification of an official photo ID, online verification via eID, online verification via mobile signature.

(c) Legal framework and supervision/governance:
The provisions of the Games of Chance Act provide for enhanced due diligence to prevent money laundering (e.g. for the replenishing of cash on playing cards in the case of VLT). In addition, due to the terms and conditions of play approved by the Gaming Inspectorate, a deposit limit of EUR 800 per registered gaming participant and week applies to **other electronic lotteries.**

Conclusion:
Based on the SNRA summary scenarios, which suggest moderately significant vulnerability, the framework conditions we have described here lead us to class the vulnerability of lotteries to exploitation for the purposes of money laundering as lowly significant.

Risk-mitigating measures

Pursuant to Art. 31c GSpG in conjunction with the FM-GwG, lottery licensees are subject to comprehensive due diligence obligations for the prevention of money laundering. **Classic lottery products** are sold exclusively in retail outlets (tobacconists, petrol stations, post offices, etc.) and the average stake amounts to EUR 5.50. In-payments for **other electronic lotteries** are limited to EUR 800 per registered player and week. To enable measures to be defined and implemented at an early stage, an independent money laundering officer must be appointed at the lottery licensee and a certified risk management and monitoring system for conspicuous gaming behaviour must be set up. For prevention of money laundering, regular training courses are held for (sales) staff. Winnings of EUR 1,000.10 or more are paid out in accordance with the terms and conditions of play approved by the Gaming Inspectorate exclusively at separately designated big-winnings payout offices upon presentation of an official photo ID, and winners are periodically checked against the PEP database. Without exception, payouts from **other electronic lotteries** are made only to EEA bank accounts.

Overall risk

The overall risk should be classified as **lowly significant.**

Recommendations

Further intensify cooperation between companies and authorities and provide information as promptly as possible in cases of suspected money laundering.

Provincial gaming with slot machines

General information

Provincial gaming with slot machines constitutes gambling services within the meaning of Art. 3 no. 14 of Directive (EU) 2015/849 in the form of terrestrial gaming that is carried out at a physical location, exclusively with slot machines (offline). Provincial gaming with slot machines covers games of chance which use slot machines (which are subject to a type approval procedure and which are electronically connected to a central control system of the central gaming 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)

and winnings (max. EUR 10,000; no jackpots) at fixed, publicly accessible premises (slot machine parlours with a minimum of 10 and a maximum of 50 slot machines or a maximum of three slot machines set up individually), in which no other games of chance may be offered (no live games), which are subject to official supervision to ensure compliance with the regulatory requirements imposed, with special accompanying measures to prevent gambling addiction as well as money laundering and the financing of terrorism.

Threat

Terrorist financing:
Based on the SNRA summary scenarios, the threat of slot machine gambling being abused for terrorist activities was classified as **not relevant**. In the text which follows, we will analyse the national risk.

In this respect, there is no real possibility of terrorist financing, as one cannot use electronic payment methods to gamble online or to bet or obtain a payout of winnings. Thus, no concealed payments to terrorists can take place. Payout ratios fixed in advance prevent an increase in the funds wagered in the sense of financing.

Conclusion:
Based on the SNRA summary scenarios, which suggest that the threat is not relevant, the current national data show that the financing of terrorist activities by means of provincial gaming with slot machines does not appear to be realistic and any residual risk which might exist is not relevant. In summary, this threat should be classified as not relevant.

Money laundering:
Based on the SNRA summary scenarios, the threat was classified as **moderately significant**. In the text which follows, we will analyse the national risk. Slot machine gambling poses a **lowly significant** threat of money laundering 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. In addition, all games played (as well as every wager and win) are seamlessly recorded electronically and transmitted to the central control system. Moreover, the game can only be played through the use of a **personalised player card,** which one obtains after presentation of an official photo ID.

Conclusion:
Based on the SNRA summary scenarios, which suggest a moderately significant threat, the current national data show the threat to be lowly significant.

Vulnerability

Terrorist financing:
Based on the SNRA summary scenarios, the vulnerability of slot machine gambling to exploitation for purposes of terrorist financing was classified as **not relevant.** The national vulnerability of slot machine gambling must also be classified as not **relevant.**

Conclusion:
In summary, the vulnerability of slot machine gambling for terrorist financing purposes should be classified as not relevant.

Money laundering:
Based on the SNRA summary scenarios, the vulnerability of slot machine gambling to exploitation for money laundering purposes was classified as **moderately significant.** In the text which follows, we will analyse the national vulnerability.

(a) Risk exposure:
Slot machine gambling is predominantly based on cash turnover. Money laundering could only be performed, if at all, by charging a large amount of cash to the player's card in order to then play with a small part of this amount and have the remaining cash paid out.

(b) Risk awareness:
In order to counter this risk, wherever cash is converted into gaming credits and vice versa, and where gamblers wager cumulative stakes totalling EUR 2,000 or more (with a possible maximum stake of EUR 10 per game) on a single gaming day or during several apparently related sessions, providers of provincial gaming with slot machines are required to exercise increased diligence (in particular to obtain and verify information on the origin of the funds used).

(c) Legal framework and supervision/governance:
The Games of Chance Act provides for enhanced due diligence requirements with regard to money laundering for the replenishing of cash on playing cards.

Conclusion:
Based on the SNRA summary scenarios, which suggest moderately significant vulnerability, the framework conditions we have presented here and, in particular, the fact that only small amounts can be wagered, lead us to class the vulnerability of slot machine gambling to exploitation for purposes of money laundering as lowly significant.

Risk-mitigating measures

Art. 5 para. 6 GSpG requires provincial operators of slot machines to comply *mutatis mutandis* with the rules applicable to casinos and lotteries with regard to money laundering and terrorist financing. Pursuant to Art. 31c para. 3 subpara. 1 GSpG, the identity of visitors is recorded on the basis of an official photo ID that meets the requirements of Art. 6 para. 2 subpara. 1 FM-GwG. The data of the official photo ID are recorded by means of scans or by manual entry. In addition, visitors can only play using a personalised player card. In particular, when cash is converted to gaming credits or vice versa, and in the case of cumulative wagers of EUR 2,000 or more, information on the origin of the wagered funds must be obtained and verified.

Overall risk

The overall risk should be classified as **lowly significant.**

Recommendations

Further intensify cooperation between companies and authorities and provide information as promptly as possible in cases of suspected 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 regulations under the respective provincial laws on bookmakers and totalisers. Competence for legislation and enforcement in the area of betting lies with the individual federal provinces.

Threat

Terrorist financing:
Based on the SNRA summary scenarios, the threat of betting being exploited for terrorist activities was classified as **not relevant**. The national threat is also classified as **not relevant.**

Conclusion:
In summary, the threat should be classified as not relevant.

Money laundering:
Based on the SNRA summary scenarios, the threat was classified as **significant**. In the text which follows, we will analyse the national risk. Risks exist from infiltration of the business area by criminal organisations, game manipulation/betting fraud, purchase of a winning ticket, calculated betting behaviour and anonymous betting or customers without identification. Overall, one should assume the threat to be **moderately significant**.

Conclusion:
Based on the SNRA summary scenarios, which suggest significant threat, the national data show a moderately significant threat. In summary, the threat should be classified as moderately significant.

Vulnerability

Terrorist financing:
Under the SNRA summary scenarios, the vulnerability of betting to exploitation for purposes of terrorist financing was classified as **not relevant.** National vulnerability is also classified as **not relevant.**

Conclusion:
In summary, the vulnerability of betting to abuse for purposes of terrorist financing should be classified as not relevant.

Money laundering:
Under the SNRA summary scenarios, the vulnerability of betting to exploitation for purposes of money laundering was classified as **significant.** In the text which follows, we will analyse the national vulnerability.

(a) Risk exposure:
A risk exists due to the high volume of bets, a large proportion of which are placed anonymously / without identifying the customer and through the use of cash.

(b) Risk awareness:
The risk is known to the regulators and the betting companies concerned and attempts are being made to counteract it through appropriate legislation and internal company measures.

(c) Legal framework and supervision/governance:
In addition to detailed provincial legal rules to combat money laundering, betting limits apply in 7 out of 9 provinces, with betting limits of between EUR 50 and 70 in 5 provinces and EUR 500 and 1,000 in two other provinces. Money laundering of high amounts would thus 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 patterns of customers is also systematically monitored through in-house risk monitoring and risk management.

Conclusion:

Based on the SNRA summary scenarios, which suggest significant vulnerability, the framework conditions we have presented here lead us to class the vulnerability of betting to exploitation for the purposes of money laundering as moderately significant.

Risk-mitigating measures

The respective provincial laws provide for detailed measures to combat money laundering. IT-supported monitoring systems are used to detect suspicious bets or transactions. In addition, the amounts of wagers are limited in the majority of the federal states.

Overall risk

The overall risk is classified as **moderately significant.**

Recommendations

Further intensify cooperation between companies and authorities and provide information as promptly as possible in cases of suspected money laundering.

Appendix

General information

Allocated human and financial resources pursuant to Art. 3 para. 3 no. 7 FM-GwG for the gambling sector

Territorial authority	Human resources (FTE)*	Financial resources*
Federal government	1	-
Burgenland	0.10	-
Carinthia	1	-
Lower Austria	0.14	-
Upper Austria	0.75	-
Salzburg	0.30	-
Styria	0.50	-
Tyrol	0.85	-
Vorarlberg	0.45	-
Vienna	1	EUR 190,000.00

*This is information provided by the Federal Ministry of Finance and the individual competent units of the provincial governments, based mainly on estimates due to the lack of exact quantifiability.

Sector risk assessment – Trade Sector

Brokerage of life insurance and insurance investment products
General information
The sector is a regulated industry pursuant to Art. 94 no. 76 Trade Act [*GewO*] 1994. Its inclusion under the regulations to combat ML/TF is provided for by Art. 365m1 para. 1 no. 4 GewO 1994. The enforcement reports of the trade authorities for 2019 assumed there were approx. 11,000 businesses which fell within the scope of enforcement. A risk survey is conducted every two years (for up to 40,000 companies in total). In order to simplify the procedure in the initial phase of the risk survey so far as possible, no distinction has been made to date with regard to money laundering and terrorist financing. However, this is planned for the future. The identification of risks from a criminology and typology perspective is currently mainly based on the results and advice contained in the SNRA and the NRA as well as provided by law enforcement authorities. The primary remit of the trade authorities is to monitor compliance with administrative law.
Threat
Terrorist financing: In the SNRA summary scenarios, the threat to this sector of abuse for terrorist financing purposes was considered moderately significant (2). The reasons for this are the complexity of the products and the elaborate planning required.
Money laundering: In the SNRA summary scenarios, the threat was classified as moderately significant (2). The reason is the elaborate planning necessary to use insurance for money laundering, which is why there are few cases. Taking into account the risk assessment carried out by the trade authorities, the results obtained are as follows: **Threat AT: 2** (2; for calculation, see appendix)
Vulnerability
Terrorist financing: In the SNRA summary scenarios, the vulnerability of the insurance brokerage sector was classified as lowly/moderately significant (1-2). The reason is the unattractiveness of the product for terrorist financing purposes**.**
Money laundering: In the SNRA summary scenarios, the vulnerability of insurance brokers with regard to exploitation for the purposes of money laundering was classified as lowly/moderately significant (1-2). Taking into account the risk assessment carried out by the trade authorities, the result is as follows **Vulnerability AT: 1-2** (1.5; for calculation, see appendix)

(a) Risk exposure:

So far, no scenarios have come to light that suggest the involvement of insurance brokers in the area of TF. The risk exposure can be further reduced by means of the now planned even more targeted risk survey documents, continuous further implementation of control measures, possibly linked to the imposition of sanctions provided for in the Trade Act. Another approach may be to further broaden the expertise of the trade authorities.

(b) Risk awareness:
As a part of extensive measures by the trade authority, such as risk surveys, control measures, etc., an increased awareness of the risks in this sector has been achieved.

(c) Legal framework and supervision/governance:
The sector is a regulated industry pursuant to Art. 94 no. 76 Trade Act [*GewO*] 1994. Its inclusion under the regulations to combat ML/TF is provided for by Art. 365m1 para. 1 no. 4 GewO 1994, and refers to life insurance and other services for purposes of investment; insurance agents are exempt if they do not accept money and either act as a single agent or within the scope of a sideline or a secondary trade. Pursuant to Art. 338 GewO 1994, the supervisory authority has extensive powers to carry out audits. ML/TF are covered content in the respective qualification examinations. In 2019/2020, the personnel resources used for enforcement of the ML/TF regulations amounted to 10.72 full-time equivalents for the entire sector (federal provinces, Federal Ministry of Digital and Economic Affairs) (law enforcement may be engaged if necessary, see Art. 336 para. 1 GewO 1994). In 2020, the problem arises that the district administrative authorities are also responsible for the pandemic response to COVID 19 and personnel from all areas of responsibility are involved in that work.

Risk-mitigating measures

Improvement of the risk survey, in particular identification of risk categories, continuous further implementation and development of supervision; more precise feedback regarding administrative offences; cooperation with other authorities so far as permitted in light of data protection issues.

Overall risk

= 1-2 (1.7; see appendix for calculation)

Recommendations

Improved training, increased enforcement activities, cooperation with other authorities such as the FMA and tax offices. Further recommendations of the European Commission, such as in particular with regard to on-site visits and thematic audits specifically with regard to beneficial ownership.

Office service providers, management consultants

General information

Data: Persons engaged in entrepreneurial activities referred to in Art. 2 para. 1 no. 3 point c in conjunction with Art. 3 no. 7 of the Money Laundering Directive, corresponding to certain sub-activities of the regulated trades of management consultants under Art. 94 no. 74 GewO 1994 and the independent trade of office work or office services (Art. 365m1 para. 2 no. 3 GewO 1994), insofar as they perform the activities mentioned in the Directive. Slightly more than 25,000 businesses, although this number is lower with regard to enforcement, since as a result of the evaluation of the risk survey and various control activities, it has been ascertained that many of the business owners in question are not engaged in any of the relevant activities, in particular those related to company formation, which is taken into account in the risk survey. A risk survey is conducted every two years (up to 40,000 businesses in total). In order to simplify the procedure during the initial phase of the risk survey so far as possible, no distinction has been made to date with regard to money laundering and terrorist financing. However, this is planned for the future. The identification of risks from a criminology and typology perspective is currently based primarily on the results and advice contained in the SNRA and the NRA as well as provided by law enforcement authorities. The primary remit of the trade authorities is to monitor compliance with administrative law.

Threat

Terrorist financing:
In the SNRA summary scenarios, it was determined by the European Commission that there is no preference by terrorist organisations for such operations as a means of financing, so the risk is classified as moderately significant (2).

Money laundering:
In the SNRA summary scenarios, the activities in question were identified as a typical vehicle for money laundering and a generally very significant risk (4) was seen that this sector could be exploited for money laundering. Taking into account the risk assessment carried out by the trade authorities, the following results are obtained:

Risk AT: 2 - 3 (2.6; see appendix for calculation)

Vulnerability

Terrorist financing:
Under the SNRA summary scenarios, the vulnerability of this sector was classified as significant (3).

Money laundering:
In the SNRA summary scenarios, the vulnerability of this sector with regard to exploitation for purposes of money laundering was classified as significant/very significant (3-4), in particular due to lacunae in identifying beneficial owners. Taking into account the risk assessment carried out by the trade authorities, the vulnerability is as follows:

Vulnerability AT: 2-3 (2.8; see appendix for calculation)

(a) Risk exposure:
In accordance with the statements in the SNRA, it cannot be ruled out that identification requirements can be circumvented when establishing companies or providing office services. A risk due to the size of the sector is relativised by the fact that, according to the results of the evaluation of the risk survey and various control activities, many of the trade

licence holders in question are not engaged in any of the relevant activities under the AMLD. The risk exposure can be further reduced by means of the now planned even more targeted risk survey documents, and continuous further implementation of control measures, possibly linked to the imposition of sanctions provided for in the Trade Act. Another approach may be to further broaden the expertise of the trade authorities.

(b) Risk awareness:
As a part of extensive measures by the trade authority, such as risk surveys, control measures, etc., an increased awareness of the risks in this sector has been achieved.

(c) Legal framework and supervision/governance:
The sector is a regulated industry pursuant to Art. 94 no. 76 Trade Act [*GewO*] 1994. Access to this industry requires proof of training, training includes ML/TF. The relevant activities within the meaning of the Money Laundering Directive as well as the activities of companies providing office services are subject to the provisions of the GewO 1994 regarding ML/TF. In 2019/2020, the personnel resources used for enforcement of the ML/TF regulations amounted to 10.72 full-time equivalents for the entire sector (federal provinces, Federal Ministry of Digital and Economic Affairs) (law enforcement may be engaged if necessary, see Art. 336 para. 1 GewO 1994). In 2020, the problem arises that the district administrative authorities are also responsible for the pandemic response to COVID 19 and personnel from all areas of responsibility are involved in that work.

Risk-mitigating measures

Improvement of the risk survey, in particular indication of risk categories, continuous further implementation and development of supervision; more precise feedback regarding administrative offences; cooperation with other authorities so far as permitted in light of data protection issues.

Overall risk

= 2-3 (2.7; see appendix for calculation)

Recommendations

Improved training, increased enforcement activities, cooperation with other authorities such as the FMA and tax offices. Follow the recommendations of the EC, in particular with regard to on-site audits and thematic audits specifically with regard to beneficial ownership.

Trading sector including auctioneers

General information

Data: The trading sector in Austria encompasses about 210,000 businesses. Risk-related focus is on trade in valuable goods such as gold and precious stones, jewellers, antiques trade, automotive trade, art trade, tobacco wholesale, oil trade, arms trade, cultural goods trade, etc. pursuant to Annex III Money Laundering Directive. Businesses are effectively within the scope if they generally conduct cash transactions of €10,000 or more, or engage in art trade or storage of works of art even for non-cash transactions of this size. According to the 2019 enforcement reports, slightly more than 16,000 commercial businesses are affected.
Risk surveys are carried out every two years (up to 40,000 companies in total). In order to simplify the procedure in the initial phase of the risk survey as much as possible, no

distinction has been made to date with regard to money laundering and terrorist financing. However, this is planned for the future. The identification of risks from a criminology and typology perspective is currently based primarily on the results and advice contained in the SNRA and the NRA as well as provided by law enforcement authorities. The primary remit of the trade authorities is to monitor compliance with administrative law.

Threat

Terrorist financing:
In the SNRA summary scenarios, a threat of traders being exploitated for terrorist activities was generally regarded to be present. The SNRA (staff document) specifically distinguishes between trade in art and antiques (2) on the one hand, and precious metals and precious stones (2-3) as well as other goods with a high individual value (e.g. cars, boats, jewellery) on the other (not relevant).

Money laundering:
In the SNRA summary scenarios, the threat with regard to trade in gold and diamonds was classified as very significant (4), as gold and diamonds can easily be transported across borders; here, there would be extensive money laundering structures (trade in art and antiques (2); other goods with a high individual value (4)). Taking into account the risk assessment carried out by the trade authorities, the results are as follows:

Threat AT: 2 (art, antiques); **3** (precious metal, precious stones), **2-3** (2.4 other valuable goods); see appendix for calculation.

Vulnerability

Terrorist financing:
In the SNRA summary scenarios, the vulnerability to abuse of traders trading in gold and diamonds for purposes of terrorist financing was classified as significant (3). For artefacts and antiques, vulnerability is rated significant/very significant (3-4) due to the lack of awareness regarding this risk. (Other goods with high individual value: not relevant).

Money laundering:
In the SNRA summary scenarios, the vulnerability to abuse for purposes of money laundering of traders trading in gold and diamonds was classified as significant (3).
The same risk exists here in the area of trade in luxury goods other than gold, diamonds and antiques, namely cars, jewellery or luxury yachts, for example (3). With regard to antiques and artefacts, vulnerability to abuse for money laundering is considered significant/very significant (3-4). Taking into account the risk assessment carried out by the trade authorities, the results are as follows:

Vulnerability AT: 3-4 (3.2 art, antiques); **2-3** (2.9 precious metals, precious stones); **2-3 (**2.2 other valuable goods); see appendix for calculation.

(a) Risk exposure:
A risk exists specifically in respect of trade and commerce due to the size of the sector. At present, the cash limits of €10,000 according to the AMLD continue to apply. Related transactions are also relevant factors triggering obligations on the part of traders. The risk exposure can be further reduced by means of the now planned even more targeted risk survey documents and continuous further implementation of control measures, possibly linked to the imposition of sanctions provided for in the Trade Act. Another approach may be to further broaden the expertise of the trade authorities.

(b) Risk awareness:
As a part of extensive measures by the trade authority, such as risk surveys, control measures, etc., increased awareness of the risks in this sector has been achieved.

(c) Legal framework and supervision/governance:
Trade law specifies general requirements for traders as well as registration, clean criminal records and clean bankruptcy records. Cash transactions of €10,000 or more in both purchase and sale trigger obligations. The trade authorities have full audit rights with regard to inspection of business documents and business premises on the basis of Art. 338 GewO 1994. Due to the implementation of the 5th Money Laundering Directive (EU) 2018/843 as per Federal Law Gazette 111/2019, art dealers are now also explicitly included in the group of obliged entities. In their case, inclusion now starts as from a limit of €10,000, also in the case of non-cash transactions. The wholesale tobacco trade, oil trade, arms trade, trade in cultural goods and other articles of special importance are explicitly mentioned as being at increased risk in the Trade Act (Annex 8 to the Trade Act). In 2019/2020, the personnel resources used in the enforcement of the ML/TF provisions amounted to 10.72 full-time equivalents for the entire sector (federal provinces, Federal Ministry of Digital and Economic Affairs) (law enforcement may be engaged if necessary, see Art. 336 para. 1 GewO 1994). In 2020, the problem arises that the district administrative authorities are also responsible for the pandemic response to COVID 19 and personnel from all areas of responsibility are involved in that work.

Risk-mitigating measures

Improvement of the risk survey, in particular indication of risk categories, continuous further implementation and development of supervision; more precise feedback regarding administrative offences; cooperation with other authorities so far as permitted in light of data protection issues.

Overall risk

= 2-3 (2.7 art, antiques; 2.9 precious metal, precious stones; 2.3 other); see appendix for calculation.

Recommendations

Improved training, increased enforcement activities, cooperation with other authorities such as the FMA and tax offices. Follow the recommendations of the European Commission, in particular with regard to on-site visits and thematic audits specifically on beneficial ownership.

Estate agents

General information

The sector is a regulated trade according to Art. 94 no. 35 of the Trade, Commerce and Industry Regulation Act 1994. Extensive training requirements apply for access to the trade; these also include training in the area of administrative law, thus including ML/TF. In the course of enforcement in 2019, it was determined that the number of affected businesses was about 6000. A risk survey is carried out every two years (up to 40,000 companies in total). In order to simplify the procedure in the initial phase of the risk survey as much as possible, no distinction has been made to date with regard to money laundering and terrorist financing. However, this is planned for the future. The identification of risks from

a criminology and typology perspective is currently based primarily on the results and advice contained in the SNRA and the NRA as well as provided by law enforcement authorities. The primary remit of the trade authorities is to monitor compliance with administrative law.

Threat

Terrorist financing:
In the SNRA summary scenarios, a threat of terrorist financing was seen in connection with frequent money laundering operations in which investments in real estate take place in order to conceal the illegal origin of assets. The threat of real estate agents being exploited for terrorist financing was considered very significant (4), in line with the money laundering risk.

Money laundering:
In the SNRA summary scenarios, a significant threat to this sector was identified, in combination with other sectors such as TCSP, and the threat was classified as very significant (4). Taking into account the risk assessment carried out by the trade authorities, the result is as follows

Risk AT: 3-4 (3.2; see appendix for calculation)

Vulnerability

Terrorist financing:
In the SNRA summary scenarios, vulnerability was seen as being exclusively related to money laundering operations, such that a separate analysis was dispensed with and vulnerability was classified as very significant (4).

Money laundering:
In the SNRA summary scenarios, the vulnerability of real estate agents with regard to exploitation for purposes of money laundering was classified as significant/very significant (3-4). Taking into account the risk assessment carried out by the trade authorities, the result is as follows

Vulnerability AT: 3-4 (3.1; see appendix for calculation)

Risk-mitigating measures

Improvement of the risk survey, in particular indication of risk categories, continuous further implementation and development of supervision; more precise feedback regarding administrative offences; cooperation with other authorities so far as permitted in light of data protection issues.

Overall risk

= 3 - 4 (3.1; see appendix for calculation) (Note: WKÖ assumed a moderately significant to significant risk for this sector; the calculated risk value of 3.1 - thus only just above three - confirms this tendency).

Recommendations

Improved training, increased enforcement activities, cooperation with other authorities such as the FMA and tax offices. Follow the recommendations of the EC, in particular with regard to on-site audits and thematic audits specifically on beneficial ownership.

Appendix

General information

On the following pages, the detailed risk values and their calculation are presented (AT risk figure, correction factor maximum +1, SNRA upper limit, AT risk figure lower limit; abbreviations: TF - SNRA - Terrorist Financing Threat as per SNRA 2019; TF - Trade - Terrorist Financing Threat as per Trade Authority Survey; ML - SNRA - Money Laundering Threat as per SNRA 2019; ML - Trade - Money Laundering Threat as per Trade Authority Survey; Total - Threat; Vuln. TF - SNRA - Vulnerability terrorist financing pursuant to SNRA 2019; Vulnerability TF - Trade - Vulnerability terrorist financing pursuant to survey of trade authorities; Vulnerability ML - SNRA - Vulnerability money laundering pursuant to SNRA 2019; Vulnerability ML – Trade - Vulnerability money laundering pursuant to survey of trade authorities; Vuln. tot. - Vulnerability total).

	Activity under SNRA life insurance		Activity under GewO insurance brokerage		Activity under SNRA TCSP		Activity under GewO business consultant, offices services provider
Threat TF - SNRA		2.0	Threat TF - SNRA			2.0	
Threat TF - Trade		2.0	Threat TF - Trade			2.0	
Average		2.0	Average			2.0	
Risk ML - SNRA		2.0	Risk ML - SNRA			4.0	
Risk ML - Trade		2.0	Risk ML - Trade			2.3	
Average		2.0	Average			3.2	
Risk total		2.0	Risk total			2.6	
Vul. TF - SNRA		1.5	Vul. TF - SNRA			3.0	
Vul. TF - Trade		1.5	Vul. TF - Trade			2.3	
Average		1.5	Average			2.7	
Vul. ML - SNRA		1.5	Vul. ML - SNRA			3.5	
Vul. ML - Trade		1.5	Vul. ML - Trade			2.3	
Average		1.5	Average			2.9	
Vul. total		1.5	Vul. total			2.8	
Total score		1.7	Total score			2.7	
Risk level	lowly-moderately significant		Risk level		moderately significant-significant		

	Activity under SNRA hv goods-artefacts, antiquities		Activity under GewO Commercial trade		Activity under SNRA hv assets-precious metals, stonres		Activity under GewO Commercial trade
Threat TF - SNRA		2.0	Threat TF - SNRA			2.5	
Threat TF - Trade		2.0	Threat TF - Trade			2.5	
Average		2.0	Average			2.5	
Risk ML - SNRA		2.0	Risk ML - SNRA			4.0	
Risk ML - Trade		2.0	Risk ML - Trade			2.8	
Average		2.0	Average			3.4	
Risk total		2.0	Risk total			3.0	
Vul. TF - SNRA		3.5	Vul. TF - SNRA			3.0	
Vul. TF - Trade		2.8	Vul. TF - Trade			2.8	
Average		3.2	Average			2.9	
Vul. ML - SNRA		3.5	Vul. ML - SNRA			3.0	
Vul. ML - Trade		2.8	Vul. ML - Trade			2.8	
Average		3.2	Average			2.9	
Vul. total		3.2	Vul. total			2.9	
Total score		2.7	Total score			2.9	
Risk level	lowly significant-significant		Risk level		moderately significant-significant		
	Activity under SNRA		Activity under GewO		Activity under SNRA		Activity under GewO

	Activity under SNRA hv assets-other than prec.met.	Activity under GewO Commercial trade		Activity under SNRA Investment real estate	Activity under GewO Real estate broker
Threat TF - SNRA		1.0	Threat TF - SNRA		4.0
Threat TF - Trade		1.8	Threat TF - Trade		2.4
Average		1.4	Average		3.2
Risk ML - SNRA		4.0	Risk ML - SNRA		4.0
Risk ML - Trade		2.8	Risk ML - Trade		2.4
Average		3.4	Average		3.2
Risk total		2.4	Risk total		3.2
Vul. TF - SNRA		1.0	Vul. TF - SNRA		4.0
Vul. TF - Trade		1.8	Vul. TF - Trade		2.4
Average		1.4	Average		3.2
Vul. ML - SNRA		3.0	Vul. ML - SNRA		3.5
Vul. ML - Trade		2.8	Vul. ML - Trade		2.4
Average		2.9	Average		3.0
Vul. total		2.2	Vul. total		3.1
Total score		2.3	Total score		3.1
Risk level	moderately significant- significant		Risk level	significant-very significant	

Closing words

The **National Risk Assessment** is the **outcome document incorporating the joint results** of all of the authorities involved in preventing and combatting money laundering and terrorist financing in Austria. It takes **into account the constant development of the European and international legal framework** and the **country review of Austria by the FATF**. In addition to taking into account new obliged entities and changed legal requirements, the methodology is based on **quantitative and qualitative factors** illustrated by **typologies** and **case studies.**

Based on a **common template and methodology,** the members of the National Coordination Panel prepared a first draft of their sector risk assessments. The first drafts were sent to the Federal Ministry of the Interior for **purposes of comparison with operational findings.** Taking into account **feedback from the Federal Ministry of the Interior** and the **private sector,** the final drafts were prepared and consolidated into the outcome document. This is based on the **expertise of all Austrian actors** involved in preventing and combatting money laundering and terrorist financing.

The National Risk Assessment is used to **identify**, **assess**, **understand** and **mitigate** the **risks of money laundering and terrorist financing that exist domestically**.

Identification and **assessment of risks** is supported by the broad sweep of the National Risk Assessment. On the one hand, **predicate offences**, **beneficial ownership** and **anti-fraud** action indicate a **broad panorama of risks**. On the other hand, the sector risk assessments paint a **diverse picture of the risk landscape**. It should be emphasised that the risks of money laundering and terrorist financing differ in relation to individual products and services as well as between sectors.

Through its detailed presentation of the risk landscape, the National Risk Assessment also contributes to **comprehension** and implementation of **risk-mitigation** measures by obliged entities. The authorities involved have formulated recommendations for further measures to mitigate the **existing risks of money laundering and terrorist financing** on the basis of the risks they identified.

This National Risk Assessment is an **important step towards preventing money laundering and terrorist financing in** Austria. The Federal Ministry of Finance is committed to **implementing international and European standards** for combating money laundering and to the continuing **further development** of those standards along with its European and international partners.

Abbreviations

AltFG	*Alternative Financing Act* (*Alternativfinanzierungsgesetz)*
AMLD	*Anti-Money Laundering Directive*
Art.	*Article*
BAO	*Federal Fiscal Code (Bundesabgabenordnung)*
BiBuG	*Federal Act on the Accountancy Professions (Bilanzbuchhaltungsgesetz)*
BWG	*Banking Act* (*Bankwesengesetz)*
BVT	*Federal Agency for the Protection of the Constitution and Counterterrorism* (*Bundesamt für Verfassungsschutz und Terrorismusbekämpfung)*
CI	*Credit institution*
CESEE	*Central, Eastern and Southeastern Europe*
et seq.	*et sequens (and what follows)*
EU	*European Union*
EU-MPfG	*EU Mandatory Disclosure Act (EU-Meldepflichtgesetz)*
FATF	*Financial Action Task Force*
FI	*Financial insitution*
FinStrG	*Financial Penal Act* (*Finanzstrafgesetz)*
FIU	*Financial Intelligence Unit (Geldwäschemeldestelle)*
FMA	*Financial Market Authority* (*Finanzmarktaufsichtsbehörde)*
FM-GwG	*Financial Markets Anti-Money Laundering Act* (*Finanzmarkt-Geldwäschegesetz)*
FTE	*full-time equivalents*
GewO	*Trade Act* (*Gewerbeordnung)*
GMSG	*Common Reporting Standard Act (Gemeinsamer Meldestandard-Gesetz)*
GSPG	*Gambling Act* (*Glücksspielgesetz)*
ML	*money laundering*
MS	*Member State (of the European Union)*
NO	*Notarial Code* (*Notariatsordnung)*
Nr.	*Number*
NRA	*National Risk Assessment*
OeNB	*Austrian Central Bank* (*Oesterreichische Nationalbank)*
para.	*paragraph*
RAO	*Lawyers' Act* (*Rechtsanwaltsordnung)*
SNRA	*Supranational Risk Assessment*
SMG	*Narcotics Act* (*Suchtmittelgesetz)*
StGB	*Austrian Criminal Code (Strafgesetzbuch)*
subpara.	*subparagraph*
SWD	*Staff Working Document*
TF	*Terrorist financing*
WAG	*Securities Supervision Act* (*Wertpapieraufsichtsgesetz)*
WiEReG	*Beneficial Owner Register or Beneficial Owner Register Act* (*Wirtschaftliche Eigentümer Register bzw. Wirtschaftliche Eigentümer Registergesetz)*
WKÖ	*Austrian Chamber of Commerce* (*Wirtschaftskammer Österreich)*
WTBG	*Chartered Accountants' Act* (*Wirtschaftstreuhandberufsgesetz)*

Bundesministerium für Finanzen
Johannesgasse 5, 1010 Wien
+43 1 514 33-0
email@bmf.gv.at
bmf.gv.at