



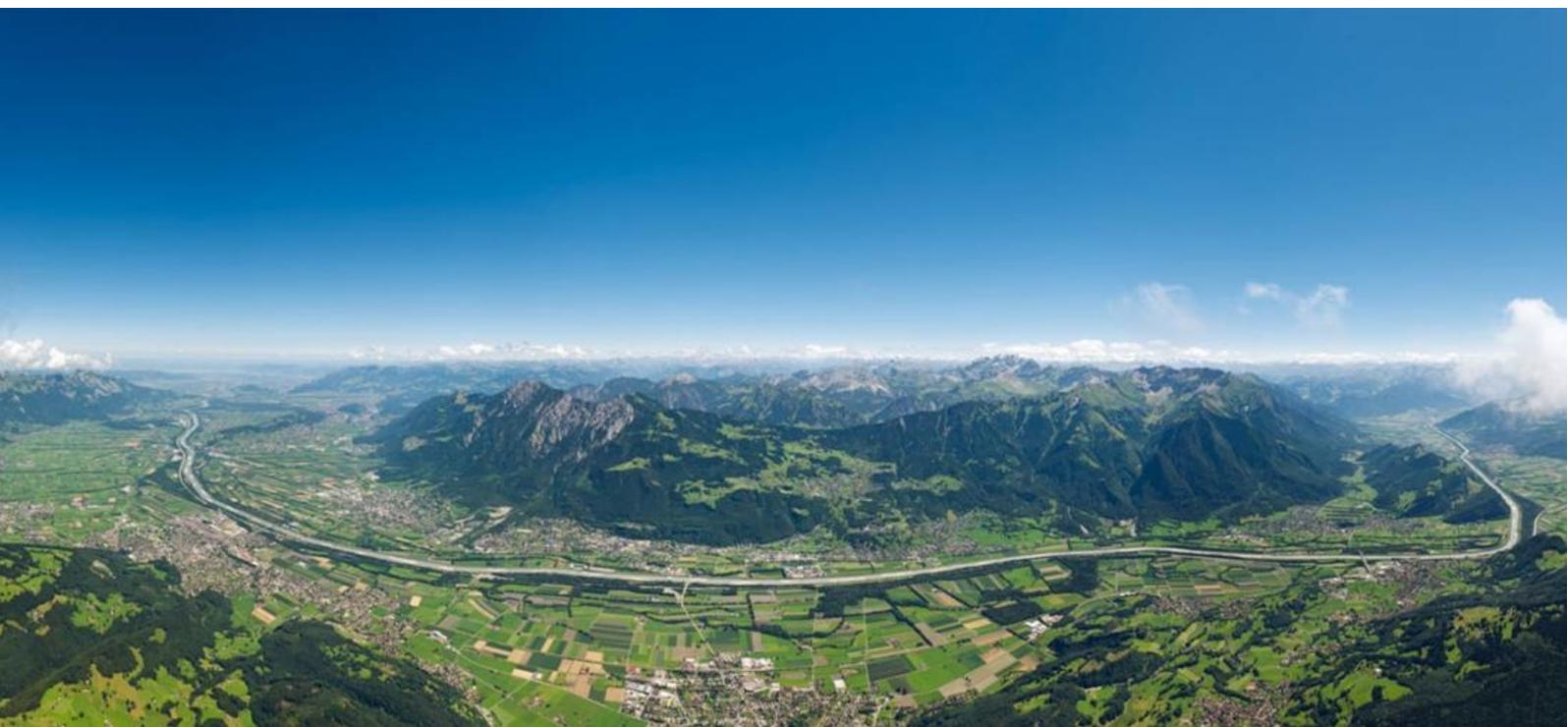
GOVERNMENT
OF THE PRINCIPALITY OF LIECHTENSTEIN

Assessment of money laundering and terrorist financing risks in the Principality of Liechtenstein

National Risk Assessment (NRA)

Summary (for publication)

July 2018



“The first step in the risk management process is to acknowledge the reality of risk. Denial is a common tactic that substitutes deliberate ignorance for thoughtful planning.”

Charles Tremper

Executive summary

Any service offered by a financial institution involves inherent risks, so that these services can in principle be misused for the purposes of money laundering and terrorist financing. Liechtenstein has pursued a consistent strategy over many years to combat this misuse. In order to combat money laundering and terrorist financing even more efficiently, the measures suitable for this purpose must in future be more risk-based than they have been in the past. Wherever increased risks exist, defensive measures must be strengthened; where the risks are assessed as low, simplified measures can be applied. This “risk-based approach” also meets the international standard for combating money laundering and terrorist financing. In order to pursue this approach, risks must first be assessed at the national level (“National Risk Assessment”). Based on this National Risk Assessment (NRA), market participants can then assess their specific risks and align their preventive measures more closely with them.

An honest and comprehensive National Risk Assessment enables the competent authorities and persons subject to due diligence to further mitigate risks and allocate resources using a risk-based approach. This includes measures by the authorities (e.g. supervisory measures), legal and regulatory measures (e.g. procedures), institutional measures (e.g. restructuring), and practical measures (e.g. training for authorities and the private sector).

The aim of this National Risk Assessment was therefore to evaluate the products and services typically offered by Liechtenstein persons subject to due diligence with regard to their exposure to risks relating to money laundering and terrorist financing. Additionally, the institutional and legal defensive measures as well as the operational and technical capacities of the competent Liechtenstein authorities were assessed. In preparing the NRA, a large volume of quantitative and qualitative data was taken into account in order to reflect the risk as precisely as possible.

The NRA concludes that – as is the case in neighbouring countries and comparable financial centres – individual business areas of the Liechtenstein financial centre, in particular private banking, financial consulting and planning (professional trustee sector), as well as the life insurance sector are exposed to heightened risks. Due to the international orientation of the financial centre, the cross-border factor is of particular importance. Furthermore, the assessment shows that heightened risks arise in particular from the predicate offences of fraud, embezzlement/criminal breach of trust, and tax offences. The analysis of vulnerabilities shows that a particular sector can in theory be seriously threatened by money laundering and terrorist financing, but the risk can be significantly reduced by appropriate and effective countermeasures.

Many of the identified risks are countered by a range of existing and implemented measures. In some areas, the authorities identified room for improvement, especially in the assessment of cross-border risks, the introduction of risk-based supervision, improvement of the efficiency of law enforcement, and the submission of suspicious activity reports.

Liechtenstein’s National Risk Assessment was prepared by the competent Liechtenstein governmental offices and the FMA and coordinated by the Financial Intelligence Unit (FIU). The operational data covers the years 2013-2015. Several measures to further limit risks were already taken in the years 2016-2017, including the introduction of the automatic exchange of information (AEOI). It is of central importance that on 1 September 2017, the revised Due Diligence Act (SPG) to implement the essential parts of the 4th EU Anti-Money Laundering Directive entered into force,

which also contains the basis for the introduction of risk-based supervision. Liechtenstein thus has a comprehensive set of legal and institutional instruments at its disposal to combat money laundering and terrorist financing.

Because this report is based on data for the years 2013-2015 and some of the changes will only take effect starting in 2018, these effects could not yet be conclusively taken into account as part of this NRA. An update of the NRA (NRA II) is therefore planned for 2019.

In July 2018, the Government approved publication of this summary in German and English.

Contents

- Executive summary 3**
- Contents..... 4**
- Introduction 5**
- 1. Threats relating to money laundering and terrorist financing 6**
 - 1.1 Summary of threats..... 6
 - 1.1.1 Threats relating to money laundering 6
 - 1.1.2 Threats relating to terrorism and terrorist financing 7
- 2. Vulnerabilities relating to money laundering and terrorist financing 8**
 - 2.1 General remarks and need for action 8
- 3. Vulnerabilities by sector 10**
 - 3.1 Need for action relating to vulnerabilities by sector..... 10
- 4. Overall risk assessment 12**
 - 4.1 Risk assessment by sector 12
 - 4.2 Risk factors that cannot be fully assessed..... 14
 - 4.3 External risk assessment by country and predicate offence 14
- 5. Outlook 15**

Introduction

This NRA reflects the assessments and understanding of the risks relating to money laundering and terrorist financing by the Liechtenstein authorities responsible for combating money laundering and terrorist financing.

The authorities based their preparation of the NRA on the World Bank's internationally recognised tool, the World Bank NRA Methodology. Cooperation with the World Bank included the provision of the methodology; an introductory seminar at the beginning of the NRA process, in which all the authorities involved and the industry associations participated; and verification of the correct application of the methodology. Responsibility for the contents of this NRA lies with the competent authorities. The World Bank had no influence on this.

The chapters on **threats** and **national vulnerabilities** were prepared exclusively within the National Administration, given that they are predominantly based on official data. The **sector-specific vulnerabilities** were developed with the participation of representatives of the respective industry associations and individual persons subject to due diligence. This process revealed commonalities in the understanding of risks, but also differences in assessing the need for further measures to mitigate these risks.

Methodology

The methodology used is based on the approach recommended by the Financial Action Task Force (FATF) on risk assessment. In a first phase, the aim is to identify threats from existing qualitative (e.g. assessments by authorities, trends, and information from other authorities) and quantitative data (e.g. number of cases of suspicion, criminal proceedings initiated, charges, convictions, incoming and outgoing requests for mutual legal assistance, police data). The threat thus constitutes only an indicator of a possible risk in the area being examined.

1. Threats relating to money laundering and terrorist financing

1.1 Summary of threats

1.1.1 Threats relating to money laundering

Threats according to predicate offence



Figure 1: Threats according to predicate offence

The threat assessment shows that the greatest threats arise from the predicate offences of fraud, criminal breach of trust/embezzlement, corruption, and bribery. This finding is based on the insights gained from operational data, which indicate that these types of cases usually involve substantial assets and, with respect to corruption/bribery, often also politically exposed persons (PEPs). These factors increase the reputation risk for the Liechtenstein financial centre. If such offences remain undetected and are not prosecuted, the impact would not be limited to the immediate effects of money laundering but would also extend to the financial centre as such (even including the initiation of criminal proceedings by foreign authorities against Liechtenstein persons subject to due diligence) and the export industry. These effects could also, under certain circumstances, lead to substantial losses of earnings for the private sector and thus also to lost tax revenue for the state. Although the consequences of such developments are difficult to assess, a negative correlation should be assumed

in principle. It must also be expected that a further consequence would be “overregulation” of the financial centre. Finally, this might provide incentives for market participants and clients to shift to unregulated or less regulated financial centres.

Threats according to sector

A heightened threat potential can be identified in the banking sector (private banking) and, to a somewhat lesser extent, in the sector of trust and company service providers (TCSPs) as well as certain life insurance products. This threat potential arises in particular due to the cross-border nature of the business model and the dependence on “introduced business” that still exists in some cases. The supranational risk assessment for the EEA region (“SNRA”) also provides evidence of the risks in these sectors, as do the assessments of other comparable financial centres.

1.1.2 Threats relating to terrorism and terrorist financing



Figure 2: Threats relating to terrorism and terrorist financing

With regard to the threat relating to terrorism and terrorist financing, it should be emphasised that – even though attacks with a terrorist background took place in German-speaking countries and in neighbouring Europe during the period under review and in the months preceding the conclusion of this report – the threat situation continues to be low with regard to attacks planned in Liechtenstein.

Neither operational data nor information from foreign partner authorities or public sources suggest the commission of a terrorist attack in Liechtenstein by domestic or foreign groups or individual perpetrators.

The situation is similar for terrorist financing, although – as explained at the outset – the threat potential arising from terrorist financing is difficult to assess on the basis of the data currently available. Especially in the area of non-profit organisations (NPOs), the authorities lack a holistic assessment of the sector and of the potential threats it poses. Terrorist financing cases from neighbouring countries in particular show that even international financial centres cannot escape responsibility in this area.¹

2. Vulnerabilities relating to money laundering and terrorist financing

2.1 General remarks and need for action

The National Risk Assessment examined the vulnerabilities in detail. The need for action to limit identified vulnerabilities at the national level can be summarised as follows.

Area	Need	Priority
Financial Market Authority	Introduction of risk-based supervision	High
Access to information from the authorities (FIU)	Direct electronic access to Commercial Register (full access)	High
FIU	Completion of the introduction of the GoAML software and database	High
Submission of suspicious activity reports	- Raising awareness of the need for immediate submission of SARs (training, updating of guidance, case-related discussions/FIU) - Sanctioning of flawed reporting behaviour	High
Convictions for money laundering/terrorist financing	- Consideration of the introduction of <i>in absentia</i> proceedings before the Criminal Court - Consideration of the introduction of easing of the burden of proof - Consideration of the inclusion of all criminal offences as predicate offences	High
Appeals to the Constitutional Court (StGH)	Limitation of individual appeals to the StGH to final decisions in the main proceedings	High
Criminal prosecution – diversion	Consideration of the abolition of diversion options for misdemeanours against the Due Diligence Act and adjustment of the relevant provisions governing criminal procedure; consideration of the amendment of the individual substantive	Medium – high

¹ See Switzerland, Mutual Evaluation Report, Financial Action Task Force, 2016, p. 78 et seq. at <http://www.fatf-gafi.org/media/fatf/content/images/mer-switzerland-2016.pdf>

	laws and elimination of the need for a final conviction in order for the Financial Market Authority (FMA) to assess trustworthiness	
Criminal prosecution – preliminary proceedings	Consideration of a switch to the investigating public prosecutor model	Medium – high
Cash controls / border controls	Consideration of options for the exchange of information with the Swiss Border Guard	Medium
National cooperation	Access to information on proceedings conducted by prosecution and supervisory authorities and the Financial Intelligence Unit (principle of reciprocity)	Medium
Terrorist financing	<ul style="list-style-type: none"> - Assessment of the vulnerability of the NPO sector and consideration of expansion of the powers of the Foundation Supervisory Authority - Further raising of market participants' awareness on the topic of terrorist financing 	Medium

3. Vulnerabilities by sector

3.1 Need for action relating to vulnerabilities by sector

Sector	Money laundering & terrorist financing risks	Mitigation of risks in practice	Need for action (general elimination of technical gaps necessary)
TCSPs	<ul style="list-style-type: none"> • Clear vulnerabilities based on product range/services offered (e.g. formation of foundations, establishments etc. for third parties, assumption of governing body mandates, formation and administration of complex structures, bearer securities etc.) • Predominantly international clients / heterogeneity of clients • High net worth individuals • Lack of risk-based supervision / deficits in dual supervision 	<p>Existing measures in principle proportionate to identified vulnerabilities, e.g.:</p> <ul style="list-style-type: none"> • Strict regulation • Functioning SPG supervision • Prudential supervision in some cases 	<ul style="list-style-type: none"> • Implementation of risk-based supervision • Optimisation of dual supervision • Improvement of system of sanctions • Increase in effectiveness of compliance function • Increase in effectiveness of system for submitting suspicious activity reports
Auditors and audit firms, auditors under business law	<ul style="list-style-type: none"> • Low vulnerabilities 	<p>Existing measures in principle proportionate to identified vulnerabilities, e.g.:</p> <ul style="list-style-type: none"> • Strict regulation • Functioning SPG supervision • Prudential supervision in some cases 	<ul style="list-style-type: none"> • Implementation of risk-based supervision • Optimisation of dual supervision • Improvement of system of sanctions • Increase in effectiveness of system for submitting suspicious activity reports
Lawyers and law firms	<ul style="list-style-type: none"> • Low vulnerabilities for lawyers and law firms subject to due diligence • Performance of TCSP activities covered by (restricted) professional trustee licence 	<p>Existing measures in principle proportionate to identified vulnerabilities, e.g.:</p> <ul style="list-style-type: none"> • Strict regulation • Functioning SPG supervision 	<ul style="list-style-type: none"> • Implementation of risk-based supervision • Optimisation of dual supervision • Improvement of system of sanctions
Real estate agents	<ul style="list-style-type: none"> • Low vulnerabilities • Strict regulation of real estate transactions 	<p>Existing measures in principle proportionate to identified vulnerabilities, e.g.:</p>	<ul style="list-style-type: none"> • Implementation of risk-based supervision • Optimisation of dual supervision

		<ul style="list-style-type: none"> • Functioning SPG supervision 	<ul style="list-style-type: none"> • Improvement of system of sanctions
Persons trading in goods	<ul style="list-style-type: none"> • Low vulnerabilities 	<p>Existing measures in principle proportionate to identified vulnerabilities, e.g.:</p> <ul style="list-style-type: none"> • Functioning SPG supervision 	<ul style="list-style-type: none"> • Implementation of risk-based supervision • Optimisation of dual supervision • Improvement of system of sanctions
Casinos and providers of online gaming	<ul style="list-style-type: none"> • Money laundering risks inherent to gaming sector as such 	<ul style="list-style-type: none"> • Comprehensive regulation • No market participants exist in this sector yet 	<ul style="list-style-type: none"> • Implementation of risk-based supervision • Optimisation of dual supervision • Improvement of system of sanctions
Value warehouses and duty-free warehouses	<ul style="list-style-type: none"> • Limited risk in light of the service offered • Limited SPG supervision 	<ul style="list-style-type: none"> • No mitigation 	<ul style="list-style-type: none"> • Establishment of adequate regulation • Implementation of risk-based supervision • Optimisation of dual supervision • Improvement of system of sanctions
Banks and other financial institutions	<ul style="list-style-type: none"> • Clear vulnerabilities based on product range/services offered (especially private banking) • Predominantly international clients • High value clients, amount of assets under management • Lack of risk-based supervision / deficits in dual supervision 	<p>Existing measures in principle proportionate to identified vulnerabilities, e.g.:</p> <ul style="list-style-type: none"> • Strict and comprehensive regulation • Prudential supervision • Annual due diligence inspections 	<ul style="list-style-type: none"> • Implementation of risk-based supervision • Optimisation of dual supervision • Improvement of system of sanctions
Insurers	<ul style="list-style-type: none"> • Vulnerabilities based on product range/services offered (especially fund- and unit-linked life insurance, single premiums) • Predominantly international clients • High value clients • Lack of risk-based supervision / deficits in dual supervision 	<p>Existing measures in principle proportionate to identified vulnerabilities, e.g.:</p> <ul style="list-style-type: none"> • Strict regulation • Prudential supervision • Annual due diligence inspections • Core market in the EEA 	<ul style="list-style-type: none"> • Implementation of risk-based supervision • Optimisation of dual supervision • Improvement of system of sanctions
Securities &	<ul style="list-style-type: none"> • Vulnerabilities based on 	Existing measures in	<ul style="list-style-type: none"> • Implementation of

asset managers	product range and complexity of products offered <ul style="list-style-type: none"> • Predominantly international clients • Amount of assets under management • Lack of risk-based supervision / deficits in dual supervision 	principle proportionate to identified vulnerabilities, e.g.: <ul style="list-style-type: none"> • Strict regulation • Prudential supervision • Annual due diligence inspections • No acceptance of assets by asset management companies and management companies 	risk-based supervision <ul style="list-style-type: none"> • Optimisation of dual supervision • Improvement of system of sanctions
-----------------------	--	--	---

4. Overall risk assessment

4.1 Risk assessment by sector

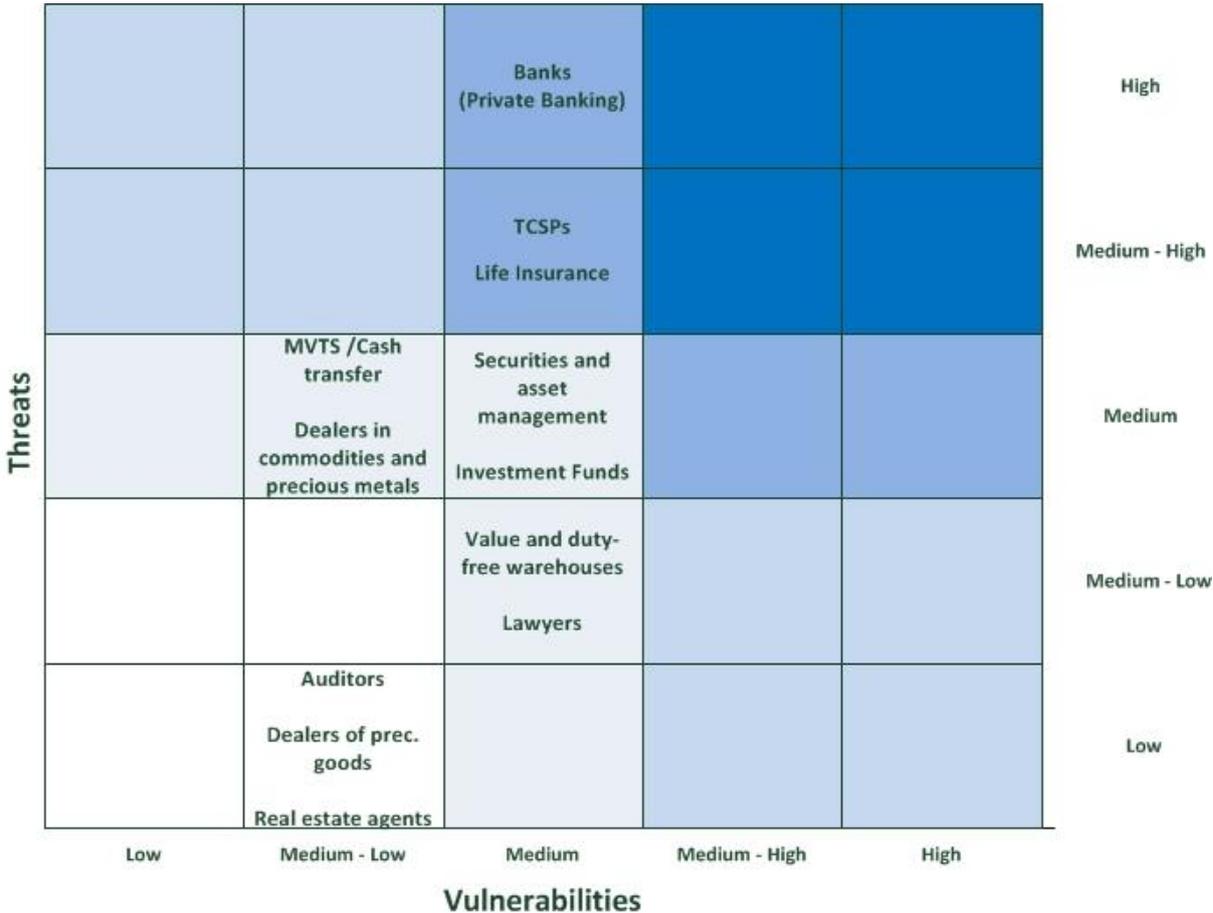


Figure 3: Sector-specific risk of money laundering and terrorist financing

The risks relating to money laundering are as follows:

In the area of banks and other financial institutions, the product range offered and the amount of assets under management generally are expected to give rise to heightened risk, especially because of the international clientele and the focus on high net worth clients and new growth markets. Other risk-increasing components include the fact that while the vast majority of suspicious activity reports were submitted by the banking sector, more than 50% of suspicious activity reports submitted during the period under review were reactive instead of proactive. Annual due diligence inspections take place alongside prudential supervision; however, the lack of risk-based supervision in private banking also had to be classified as a risk-increasing factor. Banks do apply an increased standard in many areas when implementing anti-money-laundering requirements. Existing measures to prevent and mitigate risks are therefore proportionate to the identified threat potential.

The increased threat to which TCSPs are exposed is being countered by ongoing efforts to reduce risks. However, these measures are not sufficient to significantly reduce the risk in view of the threats. In addition to banks and other financial institutions, this sector thus represents the highest risk in the Liechtenstein financial centre of being misused for the purpose of money laundering and/or terrorist financing. The most risk-increasing components here are above all:

- the international clients and the associated focus on new “growth markets” (including countries with a high risk of corruption)
- the focus on very high net worth clients
- financial consulting and planning and the associated risks in establishing the business relationship (beneficial owners and effective control)
- deficits in reporting behaviour in cases of suspicion and the plausibility check of complex transactions
- lack of comprehensive risk-based supervision

Similar deficits in risk mitigation can be seen in life insurance. However, it must be pointed out that the heightened risk is limited to certain life insurance products. Most significant in this regard is that a wide range of asset types can be invested in life insurance policies. In practice, it has repeatedly been seen that many different kinds of assets paid in to life insurance policies may originate from criminal activities or may be associated with money laundering or predicate offences to money laundering. The advantage of these financial instruments is that the identity of the beneficial owner is known only to the company offering life insurance. In the case of single premiums in particular, the effectiveness of the transaction monitoring system under the SPG is proving to be limited if there are no indications of the criminal origin of assets at the time when they were paid in. As a rule, new verification of the persons involved with regard to indicators of money laundering, predicate offences to money laundering, and other predicate offences takes place only at the time when redemption is requested or when a claim arises.

The securities/asset managers/funds sector also exhibits heightened risk. In the view of the authorities, the current qualification of vulnerability is based on data and experiences whose quality is still insufficient. The market trends relating to single investor funds under the Investment Undertakings Act (IUG) still appear to be unfamiliar. It cannot be ruled out that single investor fund structures may be used deliberately to conceal assets acquired through criminal offences. Like other products, they are suitable for contributing a wide range of assets (shareholdings, real estate and other tangible assets, bank accounts) and are therefore at least as interesting for money laundering

purposes. In addition, such funds can also be established by or for legal entities. As mentioned at the outset, the other sectors represent only minor threat and/or vulnerability factors, so that their associated risk should be assessed as significantly lower.

The following factors play an important role in assessing the risk of terrorist financing (TF):

Client risk:

1. Liechtenstein is a financial centre that specialises predominantly in European clients. The majority of the target countries of Liechtenstein financial institutions are countries in which the risk of terrorism is considered to be low.
2. Liechtenstein financial institutions have not had and still do not have subsidiaries or branches in countries where terrorism risk is classified as high.
3. Financial institutions from countries in which the terrorism risk is classified as high do not have branches or subsidiaries in Liechtenstein.

Product risk:

4. The main products of the Liechtenstein financial centre (asset structuring, high-end asset management, insurance, highly specialised investment funds) have a very high degree of complexity and are important only for a very high net worth clientele. These products are classified internationally as products with low TF risk.
5. Products that are classified internationally as associated with high TF risks (e.g. MSBs) are of very little significance in Liechtenstein.

Statistics likewise show that the risk of TF can be assessed as low: First, there are virtually no suspicious activity reports relating to TF. Despite the very high number of incoming FIU enquiries and requests for mutual legal assistance from abroad, there have been virtually no requests relating to TF in the last 10 years. None of the comprehensive analyses of European FIUs on foreign terrorist fighters have made any reference to Liechtenstein. Our investigations have also shown that the authorities of neighbouring countries specialising in defence against TF have not indicated any references to Liechtenstein in recent years.

4.2 Risk factors that cannot be fully assessed

Apart from NPOs, the first round of the National Risk Assessment is incomplete in its coverage of casinos (including online gaming), duty-free warehouses, free customs warehouses, and value warehouses. Casinos have only recently been licensed in the gaming sector. With respect to duty-free warehouses, free customs warehouses, and value warehouses, the underlying threats and vulnerabilities cannot yet be measured beyond doubt due to a lack of data and operational knowledge. In this sector, there is currently still a lack of adequate regulation and associated supervision.

4.3 External risk assessment by country and predicate offence

As explained in detail at the outset, the money laundering and terrorist financing risk in the Liechtenstein financial centre inherently depends heavily on external (non-domestic) factors.

Accordingly, it is advisable in future to examine countries and predicate offences which carry increased risk potential for domestic market participants.

5. Outlook

This document represents Liechtenstein's first comprehensive National Risk Assessment relating to money laundering and terrorist financing. As already explained in more detail at the outset, however, the underlying data situation was limited in certain areas. Accordingly, the results presented in the "Overall Risk Assessment" chapter should not be understood conclusively. In a second round of the National Risk Assessment, the limited data situation will be expanded. This should include in particular the following factors:

- payment flows from and to Liechtenstein (banking transactions and payment service providers) broken down by amounts/sums, currencies, and countries of origin and destination
- nationality and place of establishment of beneficial owners, in particular of banking and TCSP customers
- number of all maintained PEP relationships, including nationality and place of residence
- number, purpose, and partner relationships of Liechtenstein NPOs transferring assets abroad