FMA

Document No.: 03/2022

Publication date: 23.02.2022

# FMA CIRCULAR

# on

# Risk assessment

## FOR THE PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

February 2022

Disclaimer: This circular does not constitute a legal regulation. It is intended to serve as guidance and reflects the FMA's legal interpretation. No rights and obligations extending over and above the provisions of the law can be derived from circulars.

# TABLE OF CONTENTS

# 1 INTRODUCTION

1 The risk-based approach for the prevention of money laundering and terrorist financing means that supra-national authorities, national governments, competent authorities and obliged entities in accordance with Directive (EU) 2018/843 (the 5th Anti-Money Laundering Directive) are expected to identify, assess and understand the risks of money laundering and terrorist financing. Consequently, proportionate actions – commensurate to the level of risk entailed – must be taken for risk mitigation purposes.

2 This circular is intended as a guideline for the identification and assessment of potential risks of money laundering and terrorist financing for obliged entities as defined in the Financial Markets Anti-Money Laundering Act (FM-GwG; Finanzmarkt-Geldwäschegesetz[1]) – hereinafter referred to as "obliged entities".

3 This circular does not constitute a legal regulation. It is intended to serve as guidance and reflects the FMA's legal interpretation. No rights and obligations extending over and above the provisions of the law can be derived from circulars.

4 Obliged entities under the FM-GwG are:

- credit institutions pursuant to Article 1 para. 1 of the Austrian Banking Act (BWG[2]) and CRR-credit institutions pursuant Article 9 BWG that provide activities in Austria through a branch;
- financial institutions pursuant to Article 1 para. 2 nos. 1 to 6 BWG (MN 5);
- insurance undertakings pursuant to Article 1 para. 1 no. 1 of the Insurance Supervision Act 2016 (VAG 2016; Versicherungsaufsichtsgesetz 2016[3]) and small insurance undertakings pursuant to Article 1 para. 1 no. 2 VAG 2016 respectively within the scope of their life insurance operations (classes 19 to 22 pursuant to Annex A of VAG 2016));
- investment firms pursuant to Article 3 para. 1 of the Securities Supervision Act 2018 (WAG 2018; Wertpapieraufsichtsgesetz 2018[4]) and investment services providers pursuant to Article 4 para. 1 WAG 2018;

[1] Financial Markets Anti-Money Laundering Act (FM-GwG; Finanzmarkt-Geldwäschegesetz), published in Federal Law Gazette I No. 118/2016 as amended.
[2] Austrian Banking Act (BWG; Bankwesengesetz), published in Federal Law Gazette No. 532/1993 as amended.
[3] Insurance Supervision Act 2016 (VAG 2016; Insurance Supervision Act 2016), published in Federal Law Gazette I No. 34/2015, as amended.
[4] Securities Supervision Act 2018 (WAG 2018; Wertpapieraufsichtsgesetz 2018), published in Federal Law Gazette I No. 107/2017, as amended.

- AIFMs pursuant to Article 1 para. 5 and Article 4 para. 1 of the Alternative Investment Fund Managers Act (AIMFG; Alternative Investmentfonds Manager-Gesetz[5]) and non-EU-AIFMs pursuant to Article 39 para. 3 AIFMG;
- electronic money institutions pursuant to Article 3 para. 2 E-Geldgesetz 2010[6];
- payment institutions pursuant to Article 10 of the Payment Services Act 2018 (ZaDiG 2018; Zahlungsdienstegesetz 2018[7]);
- the Austrian Post with regard to its money transaction services;
- financial institutions pursuant to points a) to d) of Article 3 (2) of Directive (EU) 2015/849 ("4th Anti-Money Laundering Directive") with their place of incorporation in another Member State with business operations conducted through branches or branch establishments located in Austria as well as branches or branch establishments of such financial institutions that are authorised in third countries;
- wind-down units pursuant to Article 84 para. 2 of the Bank Recovery and Resolution Act (BaSAG; Bundesgesetz über die Sanierung und Abwicklung von Banken[8]) as well as Article 3 para. 4 of the Federal Act on the Creation of a Wind-down Unit (GSA; Bundesgesetz zur Schaffung einer Abbaueinheit[9]);
- wind-down entities pursuant to Article 162 para. 1 BaSAG in conjunction with Article 84 para. 2 BaSAG;
- virtual asset service providers pursuant to Article 2 no. 22 FM-GwG (point 6).

5 A financial institution pursuant to Article 1 para. 2 nos. 1 to 6 BWG is an institution that is not a credit institution as defined in Article 1 para. 1 BWG, and which is authorised to provide one or several of the activities listed in Article 1 para. 2 BWG on a commercial basis, provided that the institution conducts such activities as its principle activity. The principal activity as defined for qualifying as a financial institution is to be identified based on the overall picture arising in the specific case in hand, i.e. taking into consideration all relevant factors of both qualitative and quantitative natures as well as criteria with regard to a flexible system. In any case, a principal activity shall be assumed to exist, in the case that the activity contributes 50 % to the entity's performance.[10] In addition, the existence of a principal activity is not only to be assessed purely based on the activity's contribution to the entity's performance - i.e. a purely quantitative feature.

[5] Alternative Investment Fund Managers Act (AIFMG; Alternative Investmentfonds Manager-Gesetz), published in Federal Law Gazette I No. 135/2013, as amended.
[6] Electronic Money Act 2010 (E-Geldgesetz 2010), published in Federal Law Gazette I No. 107/2010 as amended.
[7] Payment Services Act 2018 (ZaDiG 2018; Zahlungsdienstegesetz 2018), published in Federal Law Gazette I no. 17/2018, as amended.
[8] Bank Recovery and Resolution Act (BaSAG; Bundesgesetz über die Sanierung und Abwicklung von Banken), published in Federal Law Gazette I No. 98/2014 as amended.
[9] Federal Act on the Creation of a Wind-Down Entity (GSA; Gesetz zur Schaffung einer Abbaueinheit), published in Federal Law Gazette I No. 51/2014 as amended.
[10] Supreme Administrative Court (VwGH) 10.11.2017, Ro 2017/02/0023 citing further literature.

Instead, it is the case, based on a holistic view of the case in hand based on qualitative features, about whether an activity of an undertaking is a principal activity, or whether this activity *"appears to be comparable due to its close relationship to the principal activity and due to its subordinate significance in comparison to the principal activity in accordance with public opinion"*.[11] In so doing, as part of a flexible system, the business plan and business strategy, the deployment of resources, returns, acquisitions and marketing etc. must be taken into account.[12] It should focus on whether a specific activity *"by way of its nature has an autonomous character or is purely of an ancillary nature to the undertaking's other […] activities"*.[13] It should be noted in this context that the definition is based on the commercial law interpretation of the principal activity and that an undertaking may not necessarily only have one principal activity.[14]

6 A virtual asset service provider is any natural or physical person resident/domiciled in Austria or providing a service in Austria pursuant to Article 2 no. 22 FM-GwG in relation to virtual currencies pursuant to Article 2 no.21 FM-GwG on a commercial basis for third parties. It also covers virtual asset service providers domiciled in another EU Member State or in a third country that actively offers or provides a service pursuant to Article 2 no. 22 FM-GwG in Austria.

7 When estimating the risk with regard to money laundering and terrorist financing, the obliged entities shall analyse all relevant risks, in order to be able to understand their effects on their entity. The risk assessment is the foundation for the risk-based approach with regard to the risk mitigation measures that are to be taken.

8 The risk-based approach is not, however, a "zero failure" approach. It is plausible that even though obliged entities may have taken appropriate measures to identify and minimise risks, such measures may nevertheless be misused for the purposes of money laundering and terrorist financing.

9 In 2012, the Recommendations of the Financial Action Task Force (FATF) – the international standards for the prevention of money laundering and terrorist financing were comprehensively updated. One of the most important changes is the significant extension of the risk-based approach, particularly with regard to preventive measures. While the 2003 Standards only applied the risk-based approach in certain areas of prevention of money laundering, the risk-based approach is identified in the 2012 Recommendations as forming an essential basis for the effective prevention of money laundering. The risk-based approach is now a comprehensive requirement extending across the entire scope of due diligence obligations. The allows the entities that are subject to these regulations to take measures in a more self-determined and therefore more flexible and variable approach with regard to the relevant risks; resources may therefore be deployed in a more focused manner and more efficiently.

[11] Federal Administrative Court (BVwG) 02.08.2017, W230 2150836-1 citing further literature.
[12] The corporate identity, company name and the activity advertised on the undertaking's website, may be taken into consideration in the assessment. Furthermore, it must also be taken into account, whether *"other items, other assets, another organisation and measures are necessary"* for the performance of the activity in questions (BVwG 02.08.2017, W230 2150836-1).
[13] Federal Administrative Court (BVwG) 02.08.2017, W230 2150836-1 citing further literature.
[14] In this case also Federal Administrative Court (BVwG) 02.08.2017, W230 2150836-1.

10 The implementation of the risk-based approach is therefore by no means optional, but is a requirement for the effective implementation of the requirements set out in the FM-GwG.

11 This circular contains the FMA's deliberations with regard to the basis of the risk-based approach for obliged entities: namely the risk assessment both at the level of the entity as well as at individual customer level. The information contained in this Circular are intended to act as guidance, with this document also constituting the FMA's legal view with regard to the risk assessment of the obliged entities.

12 This circular was drawn up taking into account the EBA Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849, repealing and replacing the Joint Committee Guidelines JC/2017/37, March 2021 (EBA/GL/2021/02). EBA Guidelines determine appropriate supervisory practices from EBA's perspective in the area of prevention of money laundering and terrorist financing within the European System of Financial Supervision, or how Union law should be applied in a specific area. Pursuant to Article 16(3) of the EBA Regulation[15] competent authorities and financial institutions must make every possible effort to comply with the Guidelines. Pursuant to Article 25 para. 3 FM-GwG, the FMA in required to apply Guidelines and Recommendations and other measures decided by EBA.

13 Where designations used refer to natural persons, the formulation used applies to both genders.

[15] Regulation (EU) No 1093/2010

# 2 NATIONAL RISK ASSESSMENT

14 Pursuant to Article 3 para. 1 FM-GwG a coordinating committee shall be established at the Federal Ministry of Finance (BMF) to identify, assess, understand and mitigate the risks prevailing in Austria with regard to money laundering and terrorist financing and all data protection issues in this regard as well as to develop measures and strategies for the prevention of money laundering and terrorist financing. The coordinating committee's duties shall include drawing up a national risk assessment (Article 3 para. 2 FM-GwG). The national risk assessment's main purpose is to improve the system for combating money laundering and terrorist financing, with the intention, in this regard, to ensure that obliged entities receive adequate information, to be able to undertake their own assessment regarding the risk of money laundering and terrorist financing more easily (Article 3 para. 3 no. 6 FM-GwG).

15 Obliged entities, when conducting their own company-level risk assessment pursuant to Article 4 para. 1 FM-GwG, must take the findings of the national risk assessment (Article 3 FM-GwG) and the European Commission's Report on the risks of money laundering and terrorist financing within the internal market pursuant to Article 6 (1) of the 4th Anti-Money Laundering Directive (Supra-national Risk Assessment) into account.

## 2.1 Introduction

16 For the purposes of this circular, the following remarks refer to Austria's National Risk Assessment of money laundering and terrorist financing (publication date: 11.05.2021). It is intended to illustrate by means of examples what relevant findings obliged entities may extract from them, so that they may subsequently use these findings in their own company-level risk assessment.

## 2.2 Contents

17 The national risk assessment on the one hand identifies and evaluates "Threats and Factors Constituting a Threat", that have been derived from criminal activities (e.g. predicate offences) and certain phenomena. On the other hand, potential "weaknesses" in the national system for the prevention of money laundering and terrorist financing are identified and assessed based on political, economic, social, technological and legislative factors, and a series of measures (priorities and strategies) defined for effectively combating money laundering and terrorist financing. The findings and measures identified in relation to these factors shall be taken into account accordingly by the obliged entities, as relevant. The national risk assessment uses the methodology of the Supra-national Risk Assessment (SNRA) as a guide for the risk assessment, and defines overall risk as:

| Overall risk = 40 % threat + 60 % vulnerability - risk-mitigating measures |
|---|

## 2.3 Predicate offences, methodologies, threats and risks

18 The National Risk Assessment contains lists and analyses of specific predicate offences and money laundering methodologies, the threats and risks in relation to money laundering, financing of terrorism and proliferation. An overview is provided hereafter.[16]

19 The most frequent predicate offences to money laundering are:

- Fraud-based criminality
- Extortion
- Narcotics-related criminality
- Organised crime
- Human trafficking and smuggling

20 The following threats in particular should be highlighted in relation to money laundering:

- Fraud and smuggling in the customs sector (overall risk: moderately significant)
- Predicate tax offences such as evasion of duties and smuggling (overall risk: moderately significant)
- Fraud with offshore links (overall risk: very significant)
- Virtual currencies and cryptoassets (overall risk: very significant)

21 The most frequently used methodologies for laundering money, are the following:

- Cryptocurrencies
- Money Mules[17]
- Hawala[18]

[16] For further details and remarks, see p. 8 et seq. of the National Risk Assessment.

[17] *"An illegal financial agent or money mule is a person who is recruited by criminals in order to launder funds obtained by illicit means. The perpetrators attempt to recruit unwitting victims with the offer of jobs as financial agents that appear to be legal. …then a sum of money is transferred to the financial agent's account from abroad, and they are then instructed to either transfer this amount of money onwards or to withdraw it from the account. The person is allowed to retain an agreed fee as remuneration. When they are instructed to make a cash withdrawal either a meeting is arranged with an unknown person, who receives the "laundered" money, or the financial agent is requested to send the money on by post or through alternative payment service providers. Criminals often choose people as potential financial agents who are new to a country, are unemployed, students or people in precarious financial situations. …"* #DontbeaMule – lass Dich nicht zum Täter machen! (Bundeskriminalamt.at) (Available in German only).

[18] *"HAWALA is a worldwide informal transaction system whose roots lie in the Eastern world. ... it is based on trust, which is formed by common linguistic, ethnic and religious similarities. This system continues even in the Internet age, where online banking is prevalent. In general, it is frequently used by people with a migration background and their family members how have stayed in their country of origin, especially in developing and crisis areas, for so-called "remittances" (transfers back to their home countries). It can be used to transfer money quickly and anonymously, even to remote areas without a corresponding infrastructure and connection to international payment transactions.* Interpol frequently defines HAWALA as "transferring of funds without actual movement of money." "The HAWALA system is suitable for criminal purposes "...because of the anonymity and the naturally minimal records as well as the often missing "paper trail" inherent in the HAWALA system..."; Geldwaesche_17_web.pdf (bundeskriminalamt.at) in German only.

- Counterfeiting of legal documents

22 The following threat scenarios should be highlighted in conjunction with terrorist financing:

- Fundraising - Donations
- Transfers to third countries

23 A risk also exists for Austrian institutions in conjunction with the financing of proliferation. The danger that weapons of mass destruction, carrier systems, dual-use goods and corresponding know-how falls into the possession of sanctioned regimes or terrorist organisations or that certain goods are misused for a purpose relevant for proliferation in contradiction with the officially stated purpose, constitutes one of the significant dangers in relation to proliferation. In this context, Austria is not only a transit country for goods that are relevant for proliferation, but also a target country for illegal procurement activities due to its highly-developed industrial production facilities as well as the large number of small- and medium-sized enterprises, which are global leaders in their particular sub-sectors. Dual-use goods are a particularly problematic area, i.e. materials or products that may be used both in the civilian and military fields due to their highly developed status.

24 Legal persons and trusts may also be misused for the purpose of money laundering and terrorist financing. In this context, there is a detailed analysis in the National Risk Assessment by the registry authority under the Beneficial Owners Register Act (WiEReG) about the individual legals forms and their corresponding risk.

## 2.4 Statements and results in relation to the financial market

25 When assessing the individual sub-sectors (credit institutions, insurance undertakings etc.) of the financial sector in the national risk assessment, it does not constitute an absolute estimation of the specific risk of money laundering and terrorist financing in the individual (Austrian) sub-sectors. The respective assessment relates far more to the relative predisposition towards risk of a sub-sector in comparison to other sectors based on objectivised, structural risk criteria. For example, the abstract risk of money laundering and terrorist financing of Austrian credit institutions is in any cases to be considered higher than that of Austrian insurance undertakings. This, however, does not mean that the Austrian banking sector is in concrete terms subject to a high risk, or even constitutes a potential weakness.

26 An overview of the results about the individual sub-sectors of the financial sector is presented below[19]:

| Sub-sector | ML Risk | TF Risk |
|---|---|---|
| Credit balance at credit Institutions and financial institutions (CIs/FIs) | high | high |
| Investment fund management companies (KAGs; Kapitalanlagegesellschaften) – real estate investment fund management companies (Immo-KAGs; Immobilien-Kapitalanlagegesellschaften) – alternative investment fund managers (AIFMs) | moderately significant | lowly significant |
| Investment firms (IFs) and Investment services providers (ISPs) | moderately significant | lowly significant |
| Private Banking-Asset Management | moderately significant to significant | lowly significant |
| Crowdfunding | moderately significant | moderately significant for the regulated area; moderately significant to significant for the non-regulated area |
| Exchange bureaux | moderately significant | moderately significant |
| Electronic money (e-money) | moderately significant | moderately significant |
| Payment Services | high | high |
| Virtual Currencies | high | high |
| "Back-to-back" business models (trust-based loans) | high | lowly significant |
| Life insurance | lowly significant | lowly significant |
| Safe rental | moderately significant | lowly significant |
| Corporate loans | lowly significant | lowly significant |
| Consumer or micro loans | moderately significant | moderately significant to significant |
| Mortgage-backed loans | moderately significant | lowly significant |

[19] For details on the sectoral analysis for the financial sector, please see the National Risk Assessment pp. 43 et seq.

# 3 RISK ASSESSMENT AT COMPANY LEVEL

## 3.1 General and Methodology

27 Under Article 4 FM-GwG, obliged entities are required to identify, evaluate and mitigate the potential risks of money laundering and terrorist financing, to which their entity is exposed. The corresponding steps involved in the investigations and assessment must be commensurate to the nature and size of the obliged entity and must be documented in an understandable manner including their outcome. These records must be updated regularly - at least annually. The risk assessment must be made available to the FMA upon request in a generally available electronic format.

28 In simple terms: during the risk assessment at company level the following questions are required to be answered:

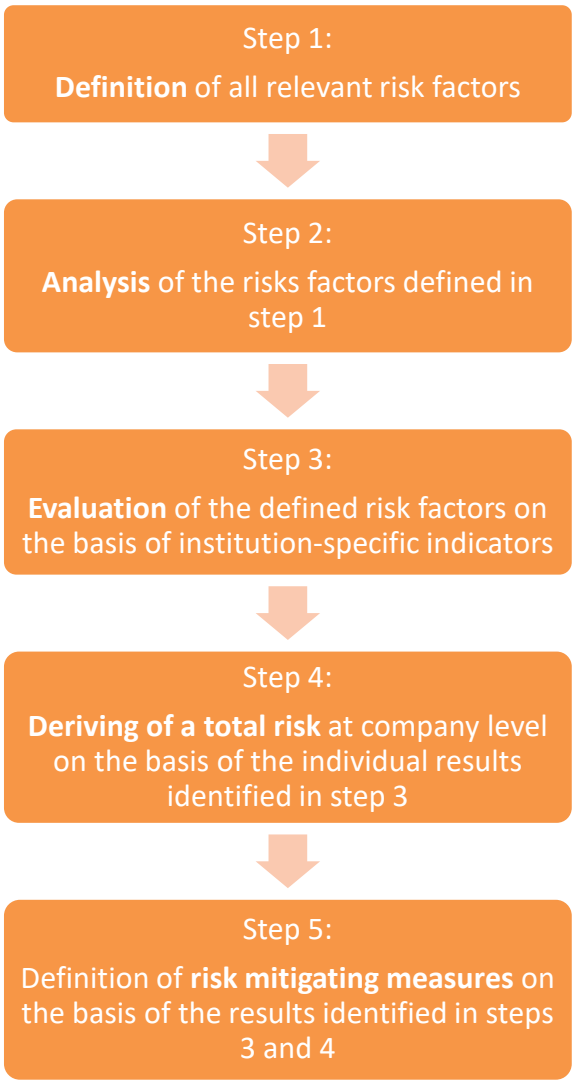
a. What relevant risk factors exist with regard to the business strategy and the institution-specific situation of the obliged entity?
b. What risk do the identified risk factors pose for the obliged entities?
c. What measures may be taken at company level to mitigate the risk accordingly?

## 3.2 Drawing up of Practical Guidelines

29 By way of introduction, with regard to the institution-specific situation, some general key figures about the entity, its business strategy (e.g. business policy and areas) as well as the business environment and the target market must be drawn up. For example, the following points should be addressed:

a. The institution's organisation (place of incorporation, total assets, number of employees, management board, supervisory board, significant holdings)?
b. In which areas are activities outsourced?
c. What does the business environment and target market look like (e.g. regional profile, profile of potential customers)?
d. What influence does the national and regulatory environment have, how has criminality developed, or what potential current phenomena exist?
e. How are the business policy and business areas (core business) set up?
f. What delivery channels exist (e.g. through qualified third parties or agents)?
g. To what extent are new technologies (such as in conjunction with customer identification) used?

30 The practical approach of the obliged entity in drawing up a corresponding risk assessment at company level can be broken down into five steps:




### 3.2.1 Step 1: Definition of all relevant risk factors

31 In the first step, the risk factors for the obliged entities must be defined that are relevant with regard to the specific institution-specific situation or the business strategy. In this regard, the EBA ML/TF Risk Factor Guidelines must also be taken into account.[20] The EU's Supra-national Risk Assessment[21], which is updated every two years, also provides valuable input for defining and analysing relevant risk factors.

32 Based on the institution-specific situation presented, all relevant risk factors must be examined for the obliged entity. As a minimum, the risk factors that are listed demonstratively in Article 4 para. 1 FM-GwG should be considered, and in particular in relation to:

[20] EBA Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849; https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/963637/Final%20Report%20on%20Guidelines%20on%20revised%20ML%20TF%20Risk%20Factors.pdf.

[21] Supranational risk assessment of the money laundering and terrorist financing risks affecting the Union (Publication date: 24 July 2019); https://ec.europa.eu/info/files/supranational-risk-assessment-money-laundering-and-terrorist-financing-risks-affecting-union_en .

a. customers,
b. countries or geographical regions,
c. products,
d. services,
e. transactions,
f. delivery channels as well as
g. any other new or developing technologies.

33 As a rule, the focus in defining these risk factors - as is also the case for the further evaluation and mitigation – shall be required to be on the specific conducted activity of the obliged entity. The risk assessment may be correspondingly brief - commensurate to the nature and size of the obliged entity, in the case that only a very narrow business segment is pursued.

### 3.2.2 Step 2: Analysis of the defined risk factors

34 In a second step, the identified risk factors are to be analysed. This means that (as a minimum) all of the risk factors listed in MN 32 as well as the respective relevant sub criteria or their significance for the assessment of the respective risk as well as the effect in general on business risk must be captured.

35 For assessing country risk, an assessment of individual countries is needed e.g. based on the level of development and the transparency of their legal system, the degree of legal clarity, the stability of their economic and political relations, the level of criminality, the stability of their financial market, the level of corruption as well as customary company registers as well as disclosure and transparency requirements. In doing so, various country lists may be referred to, cf. MN 76 and MN 93et seq. Based on this assessment, for example, countries may be split into: EU Member States, comparable third countries, high risk third countries pursuant to Article 2 no. 16 FM-GwG, countries against whom sanctions are in place, offshore countries and countries with a high degree of corruption. Offshore countries or countries with a high level of corruption are for example to be assigned a "high" risk.

36 The product risk depends on among other factors on the potential for misuse that is associated with the product offered with regard to money laundering or terrorist financing. The degree of anonymity, e.g. in the case of certain virtual currencies, the cash nature, the liquidation, the distribution channels and the complexity of the products are to be taken into consideration. The possibility of anonymous usage (e.g. using prepaid cards etc.), an increased intensity of the use of cash, the availability of liquidity at all times as well as complex products (e.g. back-to-back trust business model, derivatives, structured or leveraged products etc.) increase the risk of the misuse for the purpose of money laundering or terrorist financing in relation to the associated lack of or impeded means of control.

37 With regard to the transaction risk, a classification is performed based on the traceability or the possibility to interrupt the traceability of transactions ("paper trail"). Transactions through payable-through accounts, occasional transactions, transactions involving offshore constructions or with a high proportion of foreign payments involving countries with a heightened risk due to

the possibility of disguising such transactions or the potential anonymity of such transactions in the risks involved. Cash transactions and cross-border transactions are also to be considered as being of increased risk, in particular where the involved institutions are not required to observe comparable due diligence obligations.

38 Customer risk should be assessed in accordance with the characteristics of the customers: e.g. whether they are natural or legal persons including the beneficial owner, their place of residence or incorporation, legal form, whether they are a private banking customer, or PEPs, as well as the sector the customer belongs to (regarding the frequency of cash payments, frequency of transactions, whether cross-border aspects exist). A high risk must be assigned to complex ownership and control structures that foster the possibility of anonymising or disguising the ownership structure and/or the origin of funds, or to certain sectors, that have a high number of transactions or a high dependency on cash transactions.

39 The distribution channel risk must be assessed by taking into consideration the intensity of contact to the customer in complying with due diligence obligations for the purpose of preventing money laundering and terrorist financing. For example, an increased risk is to be assigned to distribution channels that make use of agents (cf. also MN 65 et seq. and MN 77 et seq.).

40 Furthermore, the risk must also be assessed in relation to new or developing technologies, taking into account, in accordance with FATF Recommendation 15, both risks that arise from the development of new products or business practices, as well as those that result from the using of new technologies. The risk arising from new or developing technologies must in any case already be evaluated by the obliged entities prior to rolling out the respective products or business practices.

41 Further factors that also may be meaningful in this context in relation to the risk content, may also be legal requirements, supervisory requirements, findings from suspected cases or current events.

42 The analysis of the risk factors and their sub-criteria in accordance with the principles stated in the risk assessment are required to be put in writing by the obliged entities and for example stated in the following form: *"Business relationships with an offshore link are to be considered as high risk because... The risk in relation to transactions in case is to be considered as high because...;".*

### 3.2.3 Step 3: Analysis of the defined risk factors

43 Connected to the definition and the analysis of the relevant risk factors, as a third step an evaluation of the risk factors must be conducted taking into consideration institution-specific figures. The individual risk factors are subsequently to be illustrated using corresponding institution-specific figures and data material or to be correlated and to be evaluated as an interim result. In this way the obliged entities are required to perform an evaluation of the individually identified sub-risks taking into consideration their institution-specific figures.

44 It is not, however, in any case sufficient to perform a concluding evaluation of the individual factors without previously having conducts an in-depth analysis that is illustrated with institution-

specific figures. It must be far more clearly apparent from the evaluation, for example, how many business relationships exist to customers that also at the same time fulfil the status of a PEP, and the contribution of this risk factor towards the entity or the activity of the entity. Formulated differently: there is a different effect on the evaluation of risk, in the case that 0.25 % or 10 % of the total customer stock has an offshore connection. This circumstance must be inferable and checkable from the perspective of the evaluation conducted by the obliged entity.

45 A comprehensible written record of the transaction risk assessment could, for example, take the following form: *"Approximately 0.5 % of the volume of settled transactions (which corresponds to EUR xxx) have a foreign link to countries within the EEA. Transactions in third countries accounted in the past year for only approximately 0.01 % of the processed transaction volume (corresponding to EUR xxx). The proportion of cash transactions the risk of which was generally rated as high, corresponds to approximately 0.2 % (corresponding to EUR xxx) of the processed transaction volume, and therefore plays a minor role. The transaction-related risk is therefore considered as low."*

46 The outcome of the individual risk factors must ultimately be plausible: for example if the analysis of the customer risk finds that a high percentage of the total customer stock has its place of residence/incorporation in countries with an increased risk and an additional considerable proportion of customer relations also have a connection to PEPs, then the customer risk will also have to be evaluated as being high.

### 3.2.4 Step 4: Deriving of a total risk at company level

47 As a fourth step, a (conclusive) total risk must be deduced from the partial findings. For example, in the case of the country risk being classified as low, product risk as moderately significant, transaction risk as significant, and the customer risk as moderately significant, this means that a corresponding total risk at company level must be deduced about the risk of misuse for the purposes of money laundering and terrorist financing that reflects the identified values.

### 3.2.5 Step 5: Risk mitigating measures

48 Finally, as a fifth step, what risk-oriented measures may be taken at company level to mitigate the risk accordingly must be defined or illustrated. These may, for example, cover:

a. appropriate strategies and procedures for observing due diligence obligations including their being documented in operating procedures, working documents (such as e.g. check-lists, processes for the acceptance of new customers, forms or similar documents);
b. the equipping of the function of the Anti-Money-Laundering Officer (AML Officer) with the necessary (adequate) resources and competences (e.g. involvement of the AML Officer when establishing a business relationship to high risk customers);
c. updating of the risk assessment at least once a year;
d. the collection of necessary data including the involvement of other departments as well as ensuring the quality of the data (also with regard to the level of detail of the data);
e. regular trainings for staff members as well as awareness-raising measures with regard to potential risk situations;

f. the deployment of IT systems for the prevention of money laundering and terrorist financing;
g. Conducting of checks including documenting them as part of a control plan;
h. Documenting the outcomes of the measures conducted.

# 4 RISK ASSESSMENT AT INDIVIDUAL CUSTOMER LEVEL

49 Pursuant to Article 6 para. 5 FM-GwG the obliged entities may determine the extent of the due diligence obligations listed in Article 6 paras. 1 to 3 FM-GwG on a risk-sensitive basis. When assessing the risks of money laundering and terrorist financing at least the variables set out in Annex I of the FM-GwG shall be taken into account. Every customer shall be assigned to a risk class as a result of this assessment. Obliged entities shall be required to be able to demonstrate to the FMA that the measures they have taken are appropriate in view of the risks of money laundering and terrorist financing that have been identified.

50 In order to be able to ensure as an obliged entity that any high-risk customer is recognised as such, in addition to the assessment of the risk variables listed in Annex I at least those risk variables listed in Annex III of the FM-GwG must also be taken into account, cf. MN 77. With regard to business relationships that constitute a high risk with regard to money laundering and terrorist financing, and which therefore required a correspondingly increased degree of monitoring, it shall therefore not be considered adequate only to consider the risk variables listed in Annex I when performing the risk classification.

51 So that it is possible from the point of view of an obliged entity for simplified due diligence obligations to be applied to a customer, in addition the risk variables contained in Annex II of the FM-GwG must also be incorporated into the risk assessment at customer level.

## 4.1 Identification and assessment of the risks of money laundering and terrorist financing

### 4.1.1 Drawing up of the risk profile

52 In order to be able to assess the risk that a business relationship poses with regard to money laundering and terrorist financing, obliged entities shall be required to have sufficient knowledge about the customer as well as the expected behaviour of the customer and transactions.[22] The obtaining of sufficient information about the customer shall be ensured by implementing comprehensive processes to observe the due diligence processes that are set out under law. Once the "Customer due diligence process" (CDD) has been conducted, obliged entities have sufficient knowledge about the identity of customers, about the profession that customers pursue and why they have decided to conduct a business relationship with the obliged entity.

53 The first steps that are taken by the obliged entities during the CDD allow the risk of money laundering and terrorist financing that arises from the business relationship to be analysed and ultimately to decide the scope of due diligence obligations to be applied.

[22] For the criteria to be considered, see also the EBA ML/TF Risk Factor Guidelines as well as point 3.2.1. of the EU's Supra-national Risk Assessment.

54 Based on Know-Your-Customer (KYC) information collected during the CDD, obliged entities are in a position to draw up a customer risk profile. This risk profile supports the obliged entities in deciding whether a business relationship should be established, or continued or terminated, as well as the extent to which measures should be taken.

55 Due diligence obligations pursuant to Article 6 FM-GwG must in any case be observed. The degree to which due diligence obligations apply depends on the risk attached to the respective business relationship, see MN 54. This means that the requirement relating to the nature and scope of the information that must be collected by obliged entities, and to what extent such information should be checked, increases commensurately with the risk associated with a business relationship. Consequently, this means that the extent of application of the due diligence obligations may be reduced in the case that the risk associated with the business relationship is considered to be of low significance.

56 In order to be able to ensure that the extent of the application of due diligence obligations is appropriate, risk profiles must be drawn up at the commencement of a new business relationship, and must be updated periodically or on a case-by-case basis.

### 4.1.2 Annex I

57 When assessing the risks of money laundering and terrorist financing the variables set out in Annex I of the FM-GwG shall be taken into account, cf. MN 49.

#### 4.1.2.1 Purpose of an account or a business relationship;

58 The understanding about the purpose and type of business relationship is a material and necessary factor for the classification of a customer's risk. The requirements for the obtaining and documenting of the information by the obliged entity vary depending on the purpose and type of business relationship according to the customer and the services that they make use of.

59 The more complex the business relationship, the greater the requirements for the obtaining of and written documentation of the purpose and type of the business relationship. In the case that a customer, for example does not have any (geographical) link to the obliged entity, then the reason why the customer would like to use services as a specific obliged entity should be documented. Furthermore, the obliged entities should be able to answer the following questions following customer meetings being held and to document them in writing:

a. Where the customer is an entrepreneur, what is the purpose of business that the entity pursues?
b. For what reason is this service in this specific institution being made use of?
c. Is the background of the customer and the beneficial owner consistent with the knowledge of the obliged entity about previous, current or proposed business activities, turnover and origin of funds of the customer?
d. In the case that the customer does not have a proven geographical link to the obliged entity: could the needs of the customer be better served elsewhere? Are there justifiable financial or legal reasons why the customer is requesting specific financial services?

#### 4.1.2.2 Level of assets deposited by a customer or the size of transactions undertaken

60 The risk evaluation of the level of assets to be deposited by a customer or the size of transactions undertaken may generally only be conducted as part of an overall view of the customer in conjunction with other risk factors: transactions that might appear to be especially high for a customer, may seem an everyday occurrence or of no special significance for corporate customers or particularly wealthy customers. With regard to the risk-based approach, it is therefore not expedient to define a threshold for what constitutes a "high" transaction that may be applied to all customers on an obliged entity. Instead a differentiated approach is required for different types of customers (e.g. corporate customers, SMEs, retail customers, institutional customers), the purpose and type of business relationship, the business activity of the customer, the provenance of the assets/the funds etc.

61 To be able to determine from what threshold in the case of certain customers an extraordinarily high transaction is deemed to exist, it is for example possible to undertake peer group comparisons in the supervised institution and thereby to identify, to what extent high transactions are expected among certain types of customer and sectors etc.

62 Unusually high assets or an unusually large quantity of transactions compared with the levels that may be expected from customers with a similar profile, suggest an increased level of risk.

63 The risk factor "Level of assets to be deposited by a customer or the size of transactions undertaken" is also particularly relevant with regard to the "private banking" and "wealth management" business branch. Obliged entities that offer asset management or private banking are exposed to an increased risk of being misused by customers for the purposing of disguising the origin of assets, based on the transactions that frequently are of high volumes and based on the large amount of assets managed under the umbrella of "Wealth Management".

#### 4.1.2.3 Regularity or duration of the business relationship.

64 Long-standing business relationships, during the course of which there is regular contact with the customer, potentially constitute a lower risk in terms of money laundering. This may be traced back, for example, to the obliged entity's experience gained from the business relationship with the customer (no irregularities in relation to transactions conduct, no change in circumstances that are material etc.

### 4.1.3 Annex II

65 If the application of simplified due diligence with regard to a business relationship occurs, then it is necessary, over and beyond the risk factors set out in Annex I to also consider the risk variables set out in Annex II in the risk classification: Pursuant to Article 8 para. 1 FM-GwG obliged entities may apply simplified due diligence towards customers, where they have determined on the basis of their risk assessment that only a low risk of money laundering or terrorist financing exists in certain areas. In this case, the risks relating to types of customers, geographic areas, and particular products, services, transactions or delivery channels shall be assessed and at least the factors of potentially lower risk situations set out in Annex II taken into account.

#### 4.1.3.1 Risk factors relating to customers

##### 4.1.3.1.1 Annex II no. 1 lit. a

66 Exchange-listed companies are

a. such companies, whose securities are admitted to listing on a regulated market in one or more Member States, or
b. exchange-listed companies from third countries, which are subject to disclosure obligations pursuant to a Regulation to be issued by the FMA on the basis of the power to issue Regulations pursuant to Article 122 para. 10 of the Stock Exchange Act 2018 (BörseG 2018;Börsegesetz 2018[23]) that are equivalent or comparable to those set out under Union law.

##### 4.1.3.1.2 Annex II no. 1 lit. b

67 The duties of the government are performed by the relevant bodies that form the public administration. This should be understood in a broad context, and covers both the enforcement by jurisdictional bodies as well as enforcement by the administrative bodies (in a narrower context). In both instances, both activities in relation to government administration as well as private sector administration are assigned to the public administration. In which form the respected facilities are organised currently is not of any importance. The term public administration therefore covers all types of legal persons governed by public law (corporations [regional and personal authorities], institutions, funds/foundations) as well as legal persons under private law, that are primarily equipped with governmental powers (e.g. Austro Control GmbH, RTR GmbH).

68 Furthermore, bodies and entities of the European Union with a legal personality are also covered by the term in question of public administration. Such bodies and entities may arise directly from the TEU/TFEU or the establishment of such entities may be directly prescribed in the treaties. On the other hand, such entities may also be established by the organs of the EU (such entities are usually assigned the designation of "Agencies").[24]

69 For the definition of state-owned enterprises, please refer to Article 2 no. 6 lit. g FM-GwG. According to this definition, in Austria this particularly applies to enterprises in which the Federal Government or a province holds at least 50% of the nominal capital, share capital or equity capital, or which is solely operated by the Federal Government, or which the Federal Government or a province actually controls by financial means or other economic or organisational measures. In this case, the restriction to enterprises at provincial level with a total annual turnover of greater than EUR 1 million in not relevant.

##### 4.1.3.1.3 Annex II no. 1 lit. c

70 See MN 76 in relation to customers that are resident in geographical areas of low risk pursuant to no. 3 of Annex II.

[23] Stock Exchange Act 2018 (BörseG 2018;Börsegesetz 2018), published in Federal Law Gazette I No. 107/2017, as amended.
[24] It is possible to search for such agencies and other entities can be found at https://europa.eu/european-union/about-eu/agencies_en.

#### 4.1.3.2 Risk factors relating to products, services, transactions or delivery channels:

##### 4.1.3.2.1 Annex II no. 2 lits. a - c

71 With regard to no. 2 lits. a to c of Annex II please refer to Article 2 para. 1 nos. 1 to 3 of the Life Insurance Due Diligence Regulation (LV-SoV; Lebensversicherung-Sorgfaltspflichtenverordnung): Article 2 para. 1 LV-SoV contains a list of the types of insurance contracts, to which the simplified due diligence obligations may be applied. This applies both in relation to the customers of the insurance undertaking itself (Article 2 no. 15 FM-GwG) as well as in relation to the beneficiaries of such insurance contracts (Article 7 para. 4 FM-GwG). With regard to so-called "low value contracts" listed in Article 2 para. 1 nos. 1 to 3 LV-SoV, the legal situation should be continued as was the case on the basis of Article 130 para. 1 no. 2 lits. a and b VAG 2016 up until 31.12.2016.[25]

The following insurance contracts are to be considered as so-called "low value contracts" pursuant to Article 2 para. 1 nos. 1 to 3 LV-SoV:

a. Life assurance policies for which the total premiums to be paid in the course of a year do not exceed EUR 1 200;
b. Life insurance policies where there is a payment of a one-off premium that does not exceed EUR 2 500;
c. Pension scheme policies, provided the policies neither contain an early surrender option, nor may they be used as collateral for loans.

The LV-SoV should also extend the possibility to apply simplified due diligence to insurance contracts in relation to company old-age provision in all its facets (occupational group insurance pursuant to Article 93 VAG 2016, future safeguarding pursuant to Article 3 para. 1 no. 15 lit. a of the Income Tax Act 1988 (EStG 1988; Einkommensteuergesetz 1988), pension reinsurance, severance reinsurance, insurance outsourcing severance and long service bonuses), to policies for state-sponsored retirement provision pursuant to Articles 108g et seq. EStG 1988 and policies with regard to supplementary pension insurance pursuant to Article 108b EStG 1988.[26]

##### 4.1.3.2.2 Annex II no. 2 lit. d

72 "financial inclusion" generally means the provision of banking and financial services to disadvantaged and vulnerable groups of society, such as e.g. persons with a low income, persons who are not captured by registration by the authorities, as well as persons who are only very marginally served by the formal financial sector, or who are fully excluded from it. Since it nowadays no longer possible to live in the European Union without a current account, EU Directive (EU) 2014/92/EU on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features created conditions that provide all consumers with access to a payment account. The rules under Union law have been transposed in Austria with the entry into force of the Consumer Payment Account Act (VZKG; Verbraucherzahlungskontogesetz[27]).

[25] Explanation toFederal Law Gazette II No. 1/2017 (in German), 2.
[26] Ibid.
[27] the Consumer Payment Account Act (VZKG; Verbraucherzahlungskontogesetz), published in Federal Law Gazette I No. 35/2016, as amended.

73 In the event that a consumer does not have an official photo identification document as defined in the FM-GwG available at the time of concluding a framework contract for a payment account, and if the consumer is therefore identified by an obliged entity using documents pursuant to Article 23 para. 6 VZKG, then this is to be taken into consideration as an additional risk factor. Further information about identification documents of asylum seekers, those who have been granted asylum, or foreigners without a right of residence please see the current version of the FMA Circular on Due Diligence for the Prevention of Money Laundering and Terrorist Financing in the February 2022 version, MN 65ff.

#### 4.1.3.2.3 Annex II no. 2 lit. e

74 During the transposition of Directive (EU) 2018/843 ("5th Anti-Money Laundering Directive") in the amendment by Federal Act in Federal Law Gazette I No. 62/2019, Article 46 FM-GwG that had hitherto applied was repealed, and since 01.01.2020 the FM-GwG's due diligence obligations have also been fully applicable to all e-money products.

### 4.1.3.3 Geographical risk factors:

#### 4.1.3.3.1 Annex II no. 3 lit. a

75 EU Member States and EEA States are possible evidence of a potentially low risk. This is due to the obligation of these countries to implement the 4th Anti-Money Laundering Directive (4th AMLD). Facts that potentially increase the risk in these countries must nevertheless also be taken into consideration, cf. MN 93 et seq.

#### 4.1.3.3.2 Annex II no. 3 lits. b - d

76 To evaluate the risk that is constituted by a third country with regard to money laundering and terrorist financing, referring for example to the following documents and information may provide necessary assistance:

a. The country is a member of the FATF or a FATF-style regional body (an "FSRB") e.g. MONEYVAL, Asia/Pacific Group on money laundering (APG), Grupo de Acción Financiera de Latinoamérica (GAFILAT), or similar.
b. Information is available from credible and trustworthy sources about the quality of AML/CFT checks in the jurisdiction, that also contain information about the quality of the effectively of the supervision and enforcement by the authorities. Potential sources predominantly include the mutual evaluations of the FATF or FSRBs. In addition, the International Monetary Fund's country inspections, Financial Sector Assessment Programme (FSAP) reports, as well as Organisation for Economic Co-operation and Development (OECD) reports may also be applied.
c. Information is available from credible and trustworthy sources about the scope of previous activities in relation to money laundering, such as corruption, organised criminality or fraud. Such information includes, for example Transparency International's Corruption Perceptions Index (CPI); OECD Country Reports regarding the prevention of corruption: "Country reports on the implementation of the OECD Anti-Bribery Convention"; or the UNODC World Drug Report.

d. Information is available from credible and trustworthy sources regarding the competence and effectiveness of investigative work and the judicial system of a jurisdiction to investigate predicate offences appropriately and to prosecute accordingly.
e. The political situation of the country is stable.
f. Information is available from credible and trustworthy sources regarding international cooperation as well as the exchange of information of the jurisdiction with foreign authorities. Credible sources in this regard include, for example Mutual Evaluations by the FATF or FSRBs as well as reports by the Forum on Transparency and Exchange of Information for Tax Purposes.

### 4.1.4 Annex III

77 Over and above applying the risk variables listed in Annex I, taking the risk variables in Annex III into consideration is in any case necessary for every risk classification of business relationships, as it may not otherwise be possible for the obliged entities to identify any high-risk customers as such, and to subject them to increased monitoring accordingly.

#### 4.1.4.1 Risk factors relating to customers

##### 4.1.4.1.1 Annex III no. 1 lit. a

78 Whether extraordinary circumstances exist in the business relationship may be assessed on the basis of the following factors or information among others:

a. Evidence exists that the customer is attempting to circumvent the justification of a business relationship.
b. Does the ownership and control structure of the customer appear transparent and reasonable? In the case that the ownership relationships and control structure are complex and unclear, it must be assessed whether there is a clearly identifiable financial and/or legal justification for this.
c. The customer demands the performance of complicated, unusual and unexpectedly high transactions. The transactions performed by the customer have a unusual or unexpected pattern without any apparent financial or legal purpose or well-founded commercial explanation. There are reasons to suggest that the customer is attempting to circumvent certain thresholds.
d. The customer demands unnecessary or inappropriate standards of confidentiality, KYC information are only made available reluctantly or begrudgingly, or attempts are made to conceal the type of business or business activities of the customer.
e. Company structures with off-shore components, foundations, trust arrangements, trusts or other forms (e.g. nominee shareholders), exist which do not allow the clear identification of the beneficial owner.
f. Not-for-profit associations taking into consideration the purpose of the organisation, its country of origin or country of registration and activity with payments frequently being made overseas.
g. Applications for security deposit box contracts by persons having no other business relationship with the institution.
h. Transactions that are made in conjunction with insurance companies should satisfy the principle of harmlessness. As soon as elements exist that indicate any deviation from "acceptable conduct" then the motives for them should be enquired about, and made credible. This in particular affects payment transactions made in cash and buy backs that occur under uneconomic conditions.

##### 4.1.4.1.2 Annex III no. 1 lit. b

79 Regarding the assessment of geographical territories with a high risk pursuant to no. 3 of Annex III, see the remarks in MN 76 and MNs 93 et seq.

#### 4.1.4.1.3 Annex III no. 1 lit. c

80 Although wealthy customers should not automatically be considered suspicious in relation to Money Laundering and Terrorist Financing, an increased risk exists based on the level of assets and in some cases the difficulty in justifying the origin of funds. The particular relationship of trust that exists towards wealthy private customers shall not be allowed to lead to reduced due diligence obligations. Instead, the objective risk should flow into the customer assessment and the customer monitoring.

In relation to the risk factor surrounding legal entities or legal construction that are used as instruments for private asset management, the following in particular should be included: foundations, trusts or constructions similar to trusts and special investment vehicles, in particular in the case that the beneficial owner is difficult to determine.

#### 4.1.4.1.4 Annex III no. 1 lit. d

81 In relation to entities with nominal shareholders or shares issued as bearer shares, in particular it should also be taken into consideration to what extent the determining and checking of the beneficial owners is made more difficult.

#### 4.1.4.1.5 Annex III no. 1 lit. e

82 Entities, whose business activities are strongly concentrated on cash, may constitute an increased risk, since, for example, cash that has been acquired by criminal activities, may be commingled with proceeds from a legitimate business activity, and in this way for example the assets arising from criminal activity may be paid into a bank account without the bank asking any questions.

#### 4.1.4.1.6 Annex III no. 1 lit. f

83 For more detailed statements about the risk factor "the ownership structure of the company appears unusual or excessively complex given the nature of the company's business" see MN 78b as well as MN 78e.

#### 4.1.4.1.7 Business activity/sector/business model of the customer

84 The risk factor "business activity/sector/business model of the customer" is not separately addressed in the Annexes. The list of risk factors contained in Annexes I - III does not constitute an exhaustive list, and the "sector" or "business model of the customer" must in any case also be considered in the classification of risks of business relationships.

85 The following information should be taken into account in this context:

a. Does the customer or the beneficial owner have connections to sectors that are usually associated with an increased risk of corruption, e.g. the construction industry, the pharmaceutical industry and healthcare, arms dealing and defence, the mining and extraction industry or public sector procurement?
b. Does the customer or the beneficial owner have connections to sectors that are associated with an increased risk of money laundering and terrorist financing, e.g. certain "money service businesses", casinos or trading in precious metals?
c. Does the customer or the beneficial owner have connections to a sector where the use of cash is particularly prevalent?

#### 4.1.4.1.8 Annex III no. 1 lit. g

86 The following circumstances may also be risk factors: the customer is a citizen of a third country, who applies for rights of residence or the citizenship of a Member State in exchange for the transfer of capital, the purchasing of real estate or government debt or investments in companies in this Member State;

### 4.1.4.2 Risk factors relating to products, services, transactions or delivery channels

#### 4.1.4.2.1 Annex III no. 2 lit. a

87 The risk factor listed in no. 2 lit. a of Annex III "private banking" covers the providing services to wealthy retail depositors, called "private banking". See MN 80 for statements about this issue.

#### 4.1.4.2.2 Annex III no. 2 lit. b

88 The risk of transactions or products that might favour anonymity must be taking into consideration accordingly (e.g. electronic money products e.g. prepaid (credit) cards).

#### 4.1.4.2.3 Annex III no. 2 lit. c

89 Annex III no. 2 lit. c lists non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures as factors that increase risk. As Article 6 para. 4 FM-GwG prescribes an exhaustive catalogue of safeguards for non-face-to-face operations, by applying these measures any increased risk is compensated for and the additional need to take this risk factor into consideration is therefore not necessary.

#### 4.1.4.2.4 Annex III no. 2 lit. d

90 The detection of payments received from unknown or unrelated third parties by the obliged entity is in particular relevant with regard to products or business relationships with a predictable circle or parties or persons and the resulting predictable transaction behaviour. This is in particular the case with products, where there are regular payments made by the same person(s) due to the type and state of the product: insurance premiums, savings products like e.g. building savings accounts, loan repayments, payments into accounts held by jointly owned property communities, etc.

#### 4.1.4.2.5 Annex III no. 2 lit. e

91 The products and business models listed in no. 2 lit. e of Annex III include in particular "mobile payments", "peer-to-peer payments" as well as products that are based on "Blockchain technology".

#### 4.1.4.2.6 Annex III no. 2 lit. f

92 Furthermore, risk factors may also arise as follows: e.g. transactions in relation to oil, weapons, precious metals, tobacco products, cultural goods and other articles of archaeological, historical, cultural or religious significance of or exceptional scientific value as well as in ivory and protected species;

#### 4.1.4.3 Geographical risk factors:

##### 4.1.4.3.1 Annex III no. 3 lits. a - d

93 See the remarks in MN 76 points a to f about the credible and reliable sources that may be applied with regard to the assessment of country risks about criminality, corruption, quality of prosecution etc.

94 The European Commission defines for which countries it has been determined that the national systems for the prevention of money laundering and terrorist financing have strategic deficiencies[28] in a Delegated Regulation. If the customer itself or a beneficial owner of a customer is domiciled in such a country, then in any case increased due diligence obligations are to be applied by the obliged entities. Furthermore, incoming and outgoing transactions in relation to such countries are to be indicated. For further information about this issue please see the current version of the FMA Circular on Due Diligence for the Prevention of Money Laundering and Terrorist Financing (publication date: February 2022), ;MNs 318 et seq.

Furthermore, the following circumstances indicate that an increased risk exists with regard to money laundering and terrorist financing in conjunction with a country:

a. political instability;
b. countries, against whom for example the European Union or the United Nations has/have imposed sanctions, embargos or similar measures;
c. information exists, e.g. from the media or law enforcement authorities, that countries support terrorist activities financially or otherwise or that known terrorist organisations are active in these countries.
d. the country is a so-called "tax haven"; the country has a particularly strong level of banking secrecy ("secrecy haven") or is an offshore destination, cf. MN 95 et seq.

95 Whether a specific jurisdiction is considered a “tax haven”, a “secrecy haven” or an “offshore destination”, is always the subject of a case-by-case review.

A vastly simplified definition of offshore finance is the provision of financial services by banks or similar financial services providers to non-residents for currency purposes. Where the following characteristics exist, it is generally to be assumed that a “tax haven”, a “secrecy haven” or an “offshore destination” exists:

a. in the jurisdiction in question the overwhelming majority of activity in the financial sector on both sides of the balance sheet is made available “offshore” (i.e. in the majority of cases the banks or financial services providers involved are non-resident for currency purposes);
b. transactions are initiated elsewhere and
c. the majority of the involved institutions are controlled by people who are non-resident.

96 The following additional characteristics are indications for the existence of a “tax haven”, a “secrecy haven” or an “offshore destination”:

[28] Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies, as amended.

a. they are jurisdictions with a relative large number of banks and financial institutions, that primarily conduct business relationships with non-residents for currency purposes.
b. the financial system including external assets and liabilities are disproportionate in comparison to the internal requirements of the jurisdiction and is set up with a view to financing the jurisdiction's national economy.
c. where in addition one or all of the following conditions exist:
   - low or zero taxes;
   - high standards with regard to banking secrecy and the ensuring of anonymity;
   - moderate or low regulatory standards.

### 4.1.5 Entity-specific risk factors

97 The list of risk variables contained in Annexes I, II and III of the FM-GwG is not exhaustive. Furthermore, depending on the business model, business environment, the magnitude and complexity of the business activity of an obliged entity it will also be necessary to take into consideration further entity-specific risk factors. This is particularly relevant, for example, where business relationships are established or products offered that from the perspective of the prevention of money laundering and terrorist financing constitute an increased risk, but which are considered specific with regard to the obliged entities, and which therefore are not taken into consideration in Annexes I-III.

#### 4.1.5.1 Special topic: Risk factors in the area of virtual currencies

98 In order to identify and analyse the potential risks of money laundering and terrorist financing in the area of virtual currencies, risk factors are to be considered in conjunction with the type of product (type of virtual currency; anonymous virtual currencies etc.), the business model (type of service including distribution channels), as well as the transactions (incl. technical possibilities for disguising them e.g. "mixing" etc.) (cf. "FATF-Report Virtual Assets, Red Flag Indicators of Money Laundering and Terrorist Financing", published on 14.09.2020).

99 In order to identify and analyse the potential risks of money laundering and terrorist financing in the area of virtual asset service providers, as a minimum, the following points should be taken into account:

- International standards and documents on virtual currencies and services or business activities in the field of virtual currencies (e.g. published by the FATF);
- The inherent risks of virtual currencies, e.g. their decentralised nature, global nature, lack of market clarity, anonymity etc.;
- The entity's general business environment;
- The technical developments in the field of virtual currencies, as well as the way virtual currencies' values have developed;
- The material risks in this context or the increased potential for abuse in relation to virtual currencies;
- The particular potential for abuse in relation to terrorist financing.

### 4.1.6 Weighting of risk factors

100 In the case that the obliged entity weights the risk factors when classifying the risks of customers, a substantiated assessment should be conducted about the relevance of the different risk factors within the context of the business relationship or the transaction. In practice, this may occur for example by assigning "scorings" to risk variables; an obliged entity, for example, could decide that another risk factor is less significant when the characteristics of the product that the customer wishes to use are taken into consideration.

101 The risk weights will therefore vary by product, customer or customer category as well as by obliged entity. The following should be ensures when weighting risk factors:

a. the weighting is not disproportionately influence by a single risk factor;
b. financial considerations and deliberations regarding the profit of the obliged entity (and not of the customer) shall not influence the risk rating;
c. the weighting shall not lead to a situation whereby the risk classification of a business relationship/transaction is not able to be classified as "high risk";
d. cases of application that are stipulated under law may not be repealed as a result of a company's proprietary weighting;
e. it is possible to overwrite automatically generated risk classifications on a case-by-case basis. The justification for the overruling of a risk classification should be suitably documented.

### 4.1.7 Risk classification using automated systems

102 The FMA's supervisory practices have shown that it is usual in the Austrian financial market, that the obliged entities do not develop the automated IT systems use for the risk classification of business relationships/occasional transactions themselves, but instead are purchased from external providers. In this case, it is necessary that the obliged entities have appropriate knowledge about how the system functions and how and in which manner the various risk factors can be combined or aggregated to arrive at an overall risk classification.[29]

103 Furthermore, it is necessary that the possibility exists for every obliged entity that their IT systems for risk classification and monitoring of institution-specific issues are taken into consideration. When, for example, prescribed systems are used within the group of entities, at least an evaluation of the calibration of the systems with regard to institutional specificities shall be necessary.

[29]The Risk Factor Guidelines, MN 38.

# 5 ANNEX

## 5.1 Literature[30]

- Directive (EU) 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC ("4th Anti-Money Laundering Directive").
- Directive (EU) 2018/843 of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU ("5th Anti-Money Laundering Directive").
- Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849, repealing and replacing the Joint Committee Guidelines JC/2017/37, March 2021 (EBA/GL/2021/02).
- Financial Action Task Force, Guidance for a risk-based approach – The banking sector, October 2014.
- Financial Action Task Force, International standards on combating money laundering and the financing of terrorism & proliferation – The FATF Recommendations, June 2021.
- International Monetary Fund (IMF), Enhancing Surveillance – Interconnectedness and Clusters, March 2012.
- FATF-Report Virtual Assets, Red Flag Indicators of Money Laundering and Terrorist Financing, September 2020.

*Note: Where this circular contains web links, this is done solely for information purposes. The links are guaranteed as being correct at the time of the decision passed regarding the publication of this FMA Circular.*

[30] Documents published by the Financial Action Task Force (FATF) may be downloaded from the Publications section of the FATF website at: http://www.fatf-gafi.org/.