FMA

Finanzmarktaufsicht
Liechtenstein

FMA Guideline 2013/1 on the risk-based approach under due diligence law

Guideline on the risk-based approach under the Law on Professional Due Diligence for the Prevention of Money Laundering, Organised Crime and Financing of Terrorism (Due Diligence Act; SPG) and the associated Due Diligence Ordinance (SPV).

Reference:	FMA Guideline 2013/1
Addressees:	Persons subject to due diligence under Article 3(1) and (2) of the Due Diligence Act
Publication:	Website
Issued:	4 March 2013
Entry into force:	4 March 2013
Last updated:	23 July 2021
Legal foundations:	
	Article 2(1)(h) SPG in conjunction with Article 2 SPV
	Article 3(1) and (2) SPG
	Articles 5 to 7a SPG in connection with Articles 6 to 11a SPV
	Article 8 SPG in conjunction with Article 20 SPV
	Article 9 SPG in conjunction with Article 22 SPV
	Article 9a SPG in conjunction with Article 22a SPV
	Article 10 and Annex 1 SPG in conjunction with Article 22b SPV
	Article 11 and Annex 2 SPG in connection with Articles 2, 21, and 23 SPV
	Article 11a SPG and Article 23a SPV in conjunction with Annex 4 SPV
	Article 20 SPG in connection with Article 27 SPV
	Article 21 SPG in connection with Articles 30 et seq. SPV
	Article 14 SPV
	Article 18(2) and (3) SPV
	Annex

Landstrasse 109 • Postfach 279 • 9490 Vaduz • Liechtenstein
Telefon +423 236 73 73 • Telefax +423 236 73 74 • www.fma-li.li • info@fma-li.li

FMA

Contents

1. General remarks

1.1 Risk-based approach according to FATF recommendations

A risk-based approach means that countries, public authorities, and the private sector have an understanding of the ML/TF risks to which they are exposed and apply AML/CFT measures in a manner and at a scale that ensures mitigation of those risks. The 2003 FATF Recommendations already provided that AML/CFT measures formulated by the FATF must be based on a good understanding of ML/TF risks. With the revised 2012 FATF Recommendations, the risk-based approach has become the linchpin for effective implementation of all requirements set out in the FATF Recommendations. While the 2003 Recommendations expected a risk-based approach only in certain circumstances, the new Recommendations define the risk-based approach as an overarching requirement forming the basis for effective implementation of all Recommendations.

The risk-based approach is therefore not optional, but rather a prerequisite for meeting all other requirements. A risk-based approach consists in the identification, assessment, and understanding of risks and the consistent application of AML/CFT measures that are adequate to ensure effective mitigation of those risks. The FATF Recommendations require the application of the risk-based approach at several levels.

Firstly, countries should develop a national ML/TF risk assessment to understand the full scope of ML/TF risks in the country. The results of the national risk assessment must then be communicated to the competent authorities and the private sector.

Secondly, the competent authorities must take into account the national risk assessment, but also understand the specific risks relating to their field of activity. Their actions, especially in the supervisory area, should be focused accordingly. Focusing on key areas increases the efficiency of the competent authorities' use of resources and the overall effectiveness of AML/CFT measures.

Finally, the private sector should be aware of the broader risks identified by the competent authorities, but also develop an understanding of the specificities of its business, customers, and products, and apply measures to combat money laundering and terrorist financing in a manner appropriate to this knowledge.

1.2 Risk-based approach at the European level

These FATF principles have also been enshrined in the EU Directive on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. The provisions contained in the Directive are further specified by the guidelines referred to in Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence and the factors to be considered when assessing the risk of money laundering and terrorist financing risk associated with individual business relationships and occasional transactions (hereinafter: "ML/TF Risk Factors Guidelines", EBA/GL/2021/02).

These guidelines, which must be observed by Liechtenstein persons subject to due diligence, define factors that companies must consider when assessing the money laundering and terrorist financing (ML/TF) risk in connection with their company and with a business relationship or occasional transaction with a natural person or legal person (hereinafter referred to as "client" or "customer"; this refers to the contracting party (CP) under the SPG). The guidelines also set out how companies need to adjust the scope of their customer due diligence (CDD) measures to adequately address the ML/TF risks they have identified.

The focus of these guidelines is on the risk assessment of individual business relationships and occasional transactions, but persons subject to due diligence must apply them *mutatis mutandis* when assessing ML/TF risk across their entire business in accordance with Article 8 of Directive (EU) 2015/849.

1.3 Basis and rationale for FMA Guideline

The starting point for strengthening the risk-based approach in Liechtenstein was transposition of Directive (EU) 2015/849 (4th Anti-Money Laundering Directive) into national law in 2017. Crucial in this regard are the

new obligations included in Article 9a SPG to prepare business-wide and individual risk assessments, as required under the Anti-Money Laundering Directive.

This FMA Guideline largely reproduces the European ML/TF Risk Factors Guidelines referred to in Section 1.2 and links them to the relevant national provisions in the SPG and the SPV. In some cases, a simple reference is made to the applicable statements in the guidelines. The FMA Guideline is addressed to all persons subject to due diligence under Article 3(1) and (2) SPG (hereinafter referred to as "persons subject to due diligence"), aiming to support them in their implementation of the risk-based approach, in particular in the identification and assessment of potential risks of money laundering and terrorist financing as well as in the design of the corresponding mitigation measures, and it defines the corresponding supervisory expectations.

Please note that, as the country-specific implementation of the European ML/TF Risk Factors Guidelines, the requirements of the FMA Guideline take precedence over the European guidelines should any discrepancies arise.

2. Basic principles of risk assessment

The requirements of the EU Anti-Money Laundering Directive concerning the preparation of risk assessments were implemented in Article 9a SPG. The provision contains two aspects:

a) Business-wide risk assessment ("business risk assessment"; BRA)

Under Article 9a(1) SPG, the persons subject to due diligence must conduct a risk assessment to determine and assess the risks confronting them in respect of money laundering and terrorist financing, i.e. the ML/TF risk to which the persons subject to due diligence are exposed as a whole due to the nature and complexity of their business.

b) Risk assessment of individual business relationships and occasional transactions ("customer risk assessment"; CRA)

Article 9a SPG includes an obligation to prepare a risk assessment of individual business relationships and transactions. Under Article 9a(4) SPG, the persons subject to due diligence must establish criteria to identify business relationships and transactions involving higher risks in their internal instructions, and categorise the relevant business relationships and transactions accordingly, i.e. the ML/TF risk to which the persons subject to due diligence are exposed by entering into a certain business relationship or carrying out a certain occasional transaction.

Each risk assessment must consist of two separate but interrelated steps: (1) identification of ML/TF risk factors and (2) assessment of ML/TF risk.

When assessing the overall level of residual ML/TF risk associated with their business (business risk assessment), persons subject to due diligence should consider both the level of the inherent risk and the quality of the inspections and other risk-mitigating factors.

2.1 Documentation of risk assessments

The risk assessments must be documented and kept up to date and submitted to the competent supervisory authority within the context of its monitoring role (see Article 9a(3) SPG). The records must be kept in such a way that it is possible for the persons subject to due diligence and for the supervisory authority to understand how the risk assessments were carried out and why they were conducted in a certain way.

The risk assessments also serve as a basis for inspections (see Article 38(d) SPV) and must therefore be made available to the auditors when inspections are conducted. Within the scope of the inspections, the risk assessments are checked for compliance with the legal requirements and for their appropriateness. It must be comprehensible to a third party which factors have an impact on the overall risk assessment and in what way.

2.2 Keeping risk assessments up to date

According to Article 9a(3), SPG, the risk assessment must be kept up to date.

Persons subject to due diligence must therefore have systems and controls in place to regularly review their business risk assessment and the risk assessment of their individual business relationships and transactions to ensure that their assessment of the ML/TF risk remains up to date and relevant.

These systems and controls should include the following:

- Setting a date for each calendar year when the next update of the business risk assessment update will take place, and setting a date on a risk-sensitive basis for the customer risk assessment to ensure that new or emerging risks are included. According to Article 9a(3) SPG in conjunction with Article 22a(3)

SPV, the risk assessments referred to in Article 9a(1) SPG (BRA) and Article 9a(4) SPG (CRA) must be carried out at regular intervals, at least once every three years (depending on the risk).

- Where the person subject to due diligence becomes aware before that date that a new ML/TF risk has emerged, or an existing risk has increased, this must be reflected in their customer and business risk assessment as soon as possible; and
- Carefully recording issues throughout the relevant period that could have a bearing on risk assessments, such as internal suspicious transaction reports, compliance weaknesses/failures, and intelligence from front office staff (first line of defence).

As part of this, persons subject to due diligence must ensure that they have systems and controls in place to identify emerging ML/TF risks and that they can assess these risks and, where appropriate, incorporate them into their business and customer risk assessments in a timely manner. For the points that these systems and controls should cover, see guideline 1.9 under "Title I: General Guidelines" of the ML/TF Risk Factors Guidelines. Relevant changes in the client structure or business activities are also of particular importance in this regard. The FMA understands this to mean, for example:

- a noticeable increase or decrease in the number of (new) customers in relation to the total number of business relationships, as a rule from a specific country or region;
- offering new products and services; but also
- noticeable increase in specific product/service requests from clients.

Please note that the information sources referred to in guideline 1.9 of the ML/TF Risk Factors Guidelines include, in particular, the national risk assessments and their updates.

2.3 Business risk assessment

Business risk assessments are intended to help persons subject to due diligence understand where they are exposed to ML/TF risks and in which areas of their business they should prioritise AML/CFT measures.

To this end, persons subject to due diligence should take a holistic view of the ML/TF risks to which they are exposed, by identifying and assessing the ML/TF risk associated with the products and services they offer, the geographical areas in which they operate, the clients they attract, and the transactions or delivery channels they use to serve their customers.

The persons subject to due diligence must:

- identify risk factors based on information from a variety of internal and external sources, including the sources listed in Section 2.4.4 of this Guideline;
- have regard to the relevant risk factors set out in Section 3 of this Guideline; and
- take into account wider contextual factors such as sectoral risk and geographic risk (sector and registered office of the person subject to due diligence/group locations).

The persons subject to due diligence must ensure that their business risk assessment is tailored to their business model and takes into account the factors and risks specific to the persons subject to due diligence, whether the person subject to due diligence draws up its own business risk assessment or contracts an external firm to draw up its business risk assessment or uses any model templates.

Similarly, where a person subject to due diligence is part of a group that draws up a group-wide risk assessment, the person subject to due diligence should consider whether the group-wide risk assessment is sufficiently detailed and specific to reflect the person subject to due diligence's business and the risks to which it is exposed as a result of the group's links to countries and geographical areas. If necessary, the group-wide risk assessment should be complemented accordingly. If the registered office of the group is

located in a country associated with a high risk of corruption, the person subject to due diligence should reflect this in its risk assessment even if the group-wide risk assessment stays silent on this point.

A generic ML/TF risk assessment that has not been adapted to the specific needs and business model of the person subject to due diligence, or a group-wide risk assessment that is taken over and applied unquestioningly, is unlikely to meet the requirements in Article 9a SPG.

2.3.1 Proportionality

As set out in Article 9a(6) SPG, the steps a person subject to due diligence takes to identify and assess ML/TF risk across its business must be proportionate to the nature and size of each person subject to due diligence. Small persons subject to due diligence that do not offer complex products or services and that have limited or purely domestic exposure may not need a complex or sophisticated risk assessment.

2.3.2 Implementation

After completing their business risk assessment, persons subject to due diligence must:

- make their business risk assessment available to the competent authorities upon request;
- take steps to ensure that employees understand the business risk assessment and how it affects their daily work in line with Article 32 SPV; and
- inform senior management about the results of their business risk assessment, and ensure that senior management is provided with sufficient information to understand, and take a view on, the risk to which their business is exposed.

2.3.3 Linking the business and customer risk assessments

Persons subject to due diligence must use the findings from their business risk assessment to inform their AML/CFT policies, controls, and procedures. Persons subject to due diligence must ensure that their business risk assessment also reflects the steps taken to assess the ML/TF risk associated with individual business relationships or occasional transactions. The business risk assessment should also reflect the ML/TF risk appetite of the person subject to due diligence.

Persons subject to due diligence must use the business risk assessment to inform the level or extent of initial customer due diligence that they will apply in specific situations, and to particular types of customer products, services, and delivery channels.

Customer risk assessments must inform, but are no substitute for, a business risk assessment.

Please refer to Annex 1 of this Guideline, which contains guidance for the preparation of a business risk assessment.

2.4 Risk assessment of individual business relationships and occasional transactions

Persons subject to due diligence must find out which ML/TF risks they are, or would be, exposed to as a result of entering into, or maintaining, a business relationship or carrying out an occasional transaction.

When identifying ML/TF risks associated with a business relationship or occasional transaction, persons subject to due diligence must consider relevant risk factors including who their customer is, the countries or geographical areas they operate in, the particular products, services, and transactions the customer requires and the channels the person subject to due diligence uses to deliver these products, services and transactions.

2.4.1 Initial customer due diligence

Before entering into a business relationship or carrying out an occasional transaction, persons subject to due diligence must first carry out due diligence in accordance with Article 5(1)(a) to (c) SPG. If the due diligence

obligations cannot be fulfilled, the person subject to due diligence may not enter into the business relationship or carry out the desired transaction, subject to Article 18 SPG. In any case, it must be checked whether a report must be submitted to the FIU pursuant to Article 17 SPG (see Article 5(3) SPG)).

Initial due diligence must include at least the following risk-sensitive measures:

- Identification and verification of the identity of the contracting party (Article 6 SPG);
- Identification and verification of the identity of the beneficial owner (Article 7 SPG);
- Establishment of a business profile (Article 8 SPG).

Persons subject to due diligence must adjust the extent of initial due diligence measures on a risk-sensitive basis, taking into account the findings from their business risk assessment. Where the assessment shows that the risk associated with a business relationship is low, persons subject to due diligence may apply simplified due diligence. Where the risk associated with a business relationship is heightened, persons subject to due diligence must apply enhanced due diligence.

2.4.2 Holistic view

Persons subject to due diligence must gather sufficient information so that they are satisfied that they have identified all relevant risk factors at the beginning of the business relationship and throughout the business relationship or before carrying out the occasional transaction. Where necessary, persons subject to due diligence must apply additional measures, and assess those risk factors to obtain a holistic view of the risk associated with a particular business relationship or occasional transaction.

There is no expectation that persons subject to due diligence should draw up a complete customer risk profile for occasional transactions.

2.4.3 Ongoing customer due diligence

Persons subject to due diligence must use risk-relevant information obtained during the course of the business relationship for individual risk assessment purposes.

2.4.4 Source of information

To identify ML/TF risk, persons subject to due diligence should refer to information from a variety of sources, which can be accessed individually or through commercially available tools or databases that pool information from several sources.

Persons subject to due diligence should consider the following sources of information:

- the European Commission's supranational risk assessment (https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-counter-terrorist-financing_en; see section on "Risk Assessment", SNRA Report 2017 and SNRA Report 2019)
- the European Commission's list of third countries with strategic deficiencies;
- information from governments and national authorities, such as national risk assessments, policy statements and alerts, and explanatory memorandums on relevant legislation;
- information from supervisory authorities;
- information from financial intelligence units (FIUs) and law enforcement agencies, such as threat reports, alerts and typologies; and
- information obtained as part of the initial due diligence process and ongoing monitoring.

Other sources of information are mentioned in guideline 1.31 of the ML/TF Risk Factors Guidelines. Persons subject to due diligence must determine the type and numbers of sources on a risk-sensitive basis, taking

into account the nature and complexity of their business. Persons subject to due diligence may not normally rely on only one source to identify ML/TF risks.

3. Identifying risk factors

Persons subject to due diligence must identify risk factors relating to their customers, countries or geographical areas, products and services, and delivery channels in the way set out in this Guideline, having also regard to the non-exhaustive list of factors set out in Annexes 1 and 2 of the Due Diligence Act. The availability of individual information referred to in Section 3.1 will as a rule depend on the degree of risk of the business relationship.

Persons subject to due diligence must bear in mind that the following risk factors are not exhaustive, nor is there an expectation that persons subject to due diligence will consider all risk factors in all cases.

Persons subject to due diligence must also note that some of the risk factors listed below may already qualify as indicators of money laundering, organised crime, and terrorist financing within the meaning of Annex 3 SPV in certain manifestations (e.g. adverse media reports on criminal acts, nature and behaviour of the client, or doubts about the information on identity provided) and no longer constitute merely risk factors.

3.1 Risk factors according to the general part of the ML/TF Risk Factors Guidelines

3.1.1 Customer risk factors

When identifying the risk associated with their customers, including the beneficial owners, persons subject to due diligence must consider the risk related to:

1) the customer's or beneficial owner's business or professional activity;
2) the customer's and beneficial owner's reputation; and
3) the beneficial owner's and customer's nature and behaviour, including whether this could point to increased TF risk.

Factors that may be relevant when identifying the risk associated with a customer's or beneficial owner's business or professional activity include:

a) Does the customer or beneficial owner have links to sectors that are commonly associated with higher corruption risk, such as construction, pharmaceuticals and healthcare, the arms trade and defence, the extractive industries or public procurement?

b) Does the customer or beneficial owner have links to sectors that are associated with higher ML/TF risk, for example certain money service businesses, casinos/gambling, or dealers in precious metals?

c) Does the customer or beneficial owner have links to sectors that involve significant amounts of cash?

d) Where the customer is a legal person, trust, or other type of legal arrangement, what is the purpose of their formation? What is the nature of their business?

e) Does the customer have political connections, for example, are they a politically exposed person (PEP), or is their beneficial owner or distribution recipient a PEP? Does the customer or beneficial owner/distribution recipient have any other relevant links to a PEP, for example are any of the directors of an entity PEPs and, if so, do these PEPs exercise significant control over the customer or beneficial owner? Where a customer or beneficial owner is a PEP, persons subject to due diligence must always apply enhanced due diligence in line with Article 11(4) and (4a) SPG (see Section 5.2.1 of this Guideline).

f) Does the customer or beneficial owner hold another prominent position or enjoy a high public profile that might enable them to abuse this position for private gain? For example, are they senior public officials with the ability to influence the awarding of public contracts, decision-making members of high-profile sporting bodies, or individuals who are known to influence the government and other senior decision-makers?

g) Is the customer an entity subject to enforceable disclosure requirements that ensure that reliable information about the beneficial owner is publicly available, for example public companies listed on stock exchanges that make such disclosure a condition for listing?

h) Is the customer a credit or financial institution acting on its own account from a state (or territory) with an effective AML/CFT regime and is it supervised for compliance with local AML/CFT obligations? Is there evidence that the customer has been subject to supervisory sanctions or enforcement for failure to comply with AML/CFT obligations or wider conduct requirements in recent years?

i) Is the customer a public administration or enterprise from a state (or territory) with low levels of corruption?

j) Is the information obtained about source of wealth, including occupation and business activity of the effective contributor of the assets, and the information obtained about source of funds reasonable, and is that information consistent with the totality of incoming and outgoing transactions?

The following factors may be relevant when identifying the risk associated with a customer's or beneficial owner's reputation:

a) Are there adverse media reports or other relevant sources of information about the customer, for example are there any allegations of criminality (including of course terrorism/terrorist financing) against the customer or the beneficial owner? If so, are these reliable and credible? Persons subject to due diligence should determine the credibility of allegations on the basis of the quality and independence of the source of the data and the persistence of reporting of these allegations, among other considerations. Persons subject to due diligence should note that the absence of criminal convictions alone may not be sufficient to dismiss allegations of wrongdoing.

b) Has the customer, beneficial owner or anyone publicly known to be closely associated with them had their assets frozen due to administrative or criminal proceedings or allegations of terrorism or terrorist financing? Does the person subject to due diligence have reasonable grounds to suspect that the customer or beneficial owner or anyone publicly known to be closely associated with them has, at some point in the past, been subject to such an asset freeze?

c) Does the person subject to due diligence know if the customer or beneficial owner has been the subject of a report of suspicion in the past?

d) Does the person subject to due diligence have any in-house information about the customer’s or the beneficial owner’s integrity, obtained, for example, in the course of a long-standing business relationship?

The following factors may be relevant when identifying the risk associated with a customer’s or beneficial owner’s nature and behaviour. Persons subject to due diligence must note that not all of these risk factors will be apparent at the outset; they may emerge only once a business relationship has been established:

a) Does the customer have legitimate reasons for being unable to provide robust evidence of their identity, perhaps because they are an asylum seeker?

b) Does the firm have any doubts about the veracity or accuracy of the customer’s or beneficial owner’s identity?

c) Are there indications that the customer might seek to avoid the establishment of a *permanent* business relationship? For example, does the customer look to carry out one transaction or several one-off transactions where the establishment of a business relationship might make more economic sense?

d) Is the customer's ownership and control structure transparent and does it make sense? If the customer's ownership and control structure is complex or opaque, is there an obvious commercial or lawful rationale?

e) Does the customer issue bearer shares or does it have nominee shareholders?

f) Is the client an entity classified as a shell company[1]?

g) Is there a sound reason for changes in the customer's ownership and control structure?

h) Does the customer request transactions that are complex, unusually or unexpectedly large, have an unusual or unexpected pattern, no apparent economic or lawful purpose, or lack a sound commercial rationale? Are there grounds to suspect that the customer is trying to evade specific thresholds defined by law?

i) Does the customer request unnecessary or unreasonable levels of secrecy? For example, is the customer reluctant to share due diligence information, or do they appear to want to disguise the true nature of their business?

j) Can the customer's or beneficial owner's source of wealth or source of funds be easily explained, for example through their occupation, inheritance or investments? Is the explanation plausible?

k) Does the customer use the products and services they have taken out as expected when the business relationship was first established?

l) Where the customer is resident abroad, could their needs be better serviced elsewhere? Is there a sound economic and lawful rationale for the customer requesting the type of financial service sought? Persons subject to due diligence should note that Article 16 of Directive 2014/92/EU creates a right for customers who are legally resident in the EEA to obtain a basic payment account, but this right applies only to the extent that credit institutions can comply with their AML/CFT obligations.

When identifying the risk associated with a customer's or beneficial owner's nature and behaviour, persons subject to due diligence must pay particular attention to risk factors that, although perhaps not directly specific to terrorist financing, could point to increased TF risk, in particular in situations where other TF risk factors are also present. To this end, persons subject to due diligence should consider at least the following risk factors:

a) Is the customer or the beneficial owner a person included in the lists of persons, groups and entities involved in terrorist acts and subject to restrictive measures or are they known to have close personal or professional links to persons registered on such lists (for example, because they are in a relationship or otherwise live with such a person)?

b) Does the customer carry out transactions that are characterised by incoming and outgoing fund transfers from and/or to countries where groups committing terrorist offences are known to be operating, that are known to be sources of terrorist financing or that are subject to international sanctions? If so, can these transfers be explained easily through, for example, family ties or commercial relationships?

c) Is the customer a non-profit organisation:

- whose activities or leadership been publicly known to be associated with extremism or terrorist sympathies? or

[1] Entity without real commercial business activity/function and without real substance that does not serve classical asset management.

- whose transaction behaviour is characterised by bulk transfers of large amounts of funds to states or territories associated with higher ML/TF risks and high-risk third countries?

d) Does the customer carry out transactions characterised by large flows of money in a short period of time, involving non-profit organisations with unclear links (e.g. they are domiciled at the same physical location; they share the same representatives or employees or they hold multiple accounts under the same names)?

e) Does the customer transfer or intend to transfer funds to persons referred to in (a) and (b)?

In addition to the information sources listed in Section **Fehler! Verweisquelle konnte nicht gefunden werden.** of this Guideline, persons subject to due diligence have to pay particular attention to the FATF's typologies on terrorist financing, which are regularly updated: https://www.fatf-gafi.org/publications/privatesector/documents/keyissues.html?hf=10&b=0&s=desc(fatf_releasedate)

3.1.2 Risk factors related to countries and geographical areas

When identifying the risk associated with countries and geographical areas, persons subject to due diligence must consider the risk related to:

1) the states or territories in which the customer is based or is resident and in which the beneficial owner is resident;

2) the states or territories that are the customer's and beneficial owner's registered offices; and

3) the states or territories to which the customer and beneficial owner have relevant personal or business links, or financial or legal interests.

Persons subject to due diligence must note that the nature and purpose of the business relationship, or the type of business, will often determine the relative importance of the risk factors related to states and geographical areas. For example:

a) Where the funds used in the business relationship have been generated abroad, the level of predicate offences to money laundering and the effectiveness of the legal system of a country of origin will be particularly relevant (e.g. Transparency Corruption Perceptions Index, contained in List A).

b) Where funds are received from, or sent to, countries where groups committing terrorist offences are known to be operating, persons subject to due diligence should consider to what extent this could be expected to or might give rise to suspicion, based on what the firm knows about the purpose and nature of the business relationship (e.g. Global Terrorism Index (GTI), contained in List A).

c) Where the customer is a credit or financial institution, companies should pay particular attention to the adequacy of the AML/CFT regime and the effectiveness of AML/CFT supervision in the country of domicile (e.g. FATF reports, especially Immediate Outcome 3).

d) Where the customer is an entity (including foundations, trusts, or similar legal arrangements such as fiducie, fideicomiso), persons subject to due diligence should take into account the extent to which the state (or territory) under whose law the legal arrangement, the trust, or the like has been effectively complies with international tax transparency standards (especially Common Reporting Standard).

Risk factors persons subject to due diligence should consider when identifying the effectiveness of a state's (or territory's) AML/CFT regime include:

a) Does the state (or territory) have strategic deficiencies (see Annex 4 SPV)? In those cases, persons subject to due diligence must refer to Article 11a SPG in conjunction with Section 5.2.4 of this Guideline.

b) Does the country's law prohibit the implementation of group-wide policies and procedures and in particular are there any situations in which Commission Delegated Regulation (EU) 2019/758 should be applied?

c) Is there information from more than one credible and reliable source about the quality of the country's AML/CFT controls, including information about the quality and effectiveness of regulatory enforcement and oversight? Examples of possible sources include mutual evaluation reports by the Financial Action Task Force (FATF) or FATF-style Regional Bodies (FSRBs) (a good starting point are the executive summary and key findings and the assessment of compliance with Recommendations 10, 26 and 27 and Immediate Outcomes 3 and 4), the FATF's list of high-risk and non-cooperative jurisdictions (black list and grey list), International Monetary Fund (IMF) assessments, and Financial Sector Assessment Programme (FSAP) reports. Persons subject to due diligence should note that membership of the FATF or an FSRB (e.g. Moneyval) does not, of itself, mean that the country's AML/CFT regime is adequate and effective. It should be noted that the countries listed in Annex 1 of FMA Instruction 2018/7 were assessed only for compliance with the FATF technical recommendations mentioned above, but not for their effectiveness (immediate outcomes). The list of countries contained in Annex 1 of FMA Instruction 2018/7 is therefore not suitable for assessing the effectiveness of the AML/CFT regime required here.

In the case of states that meet the criteria set out in c) above but at the same time exhibit a higher risk of corruption or terrorist financing or are affected by sanctions, embargoes, or similar measures, an overall consideration of the geographical risks must be carried out (example: State X meets the above criteria but exhibits a higher risk of corruption according to the Corruption Perceptions Index).

In such cases, the existence of the latter geographical risks (corruption risk, terrorist financing risk, sanctions) will as a rule be of greater importance than the fact that in the state concerned the AML/CFT requirements comply with the FATF Recommendations 2012 and that these requirements are effectively implemented according to country evaluation reports.

Factors that persons subject to due diligence should consider when identifying the level of terrorist financing risk associated with a country include:

a) Is there information, for example from law enforcement or credible and reliable open media sources, suggesting that a country provides funding or support for terrorist activities, either from official sources, or from organised groups or organisations within that country?

b) Is there information, for example from law enforcement or credible and reliable open media sources, suggesting that groups committing terrorist offences are known to be operating in the country or territory (e.g. Global Terrorism Index, contained in List A)?

c) Is the country subject to financial sanctions, embargoes or measures that are related to terrorism, financing of terrorism, or proliferation of weapons of mass destruction issued by, for example, the United Nations or the European Union?

Factors that persons subject to due diligence should consider when identifying a country's level of transparency and tax compliance include:

a) Is there information from more than one credible and reliable source that the country has been deemed compliant with international tax transparency and information sharing standards? Is there evidence that relevant rules are effectively implemented in practice? Examples of possible sources include reports by the Global Forum on Transparency and the Exchange of Information for Tax Purposes of the Organisation for Economic Co-operation and Development (OECD), which rate jurisdictions for tax transparency and information sharing purposes; assessments of the country's commitment to automatic exchange of information based on the Common Reporting Standard; assessments of

compliance with FATF Recommendations 9, 24 and 25 and Immediate Outcomes 2 and 5 by the FATF or FSRBs; and IMF assessments (e.g. IMF staff assessments of offshore financial centres).

b) Has the country committed to, and effectively implemented, the Common Reporting Standard on Automatic Exchange of Information, which the G20 adopted in 2014?

c) Has the jurisdiction put in place reliable and accessible beneficial ownership registers?

Risk factors persons subject to due diligence should consider when identifying the risk associated with the level of predicate offences to money laundering include:

a) Is there information from credible and reliable public sources about the level of predicate offences to money laundering, for example bribery, organised crime, tax crime, and serious fraud? Examples include corruption perception indices; OECD country reports on the implementation of the OECD's anti-bribery convention; and the United Nations Office on Drugs and Crime World Drug Report.

b) Is there information from more than one credible and reliable source about the capacity of the country's investigative and judicial system effectively to investigate and prosecute these offences?

In connection with the above-mentioned geographical risks, the FMA refers in particular to the following publications:

- Transparency International Corruption Perceptions Index (the FMA assumes a higher risk for third countries with a score of less than 50 points)
- States affected by sanctions under the ISG
- States with strategic deficiencies (see Annex 4 SPV)
- Jurisdictions that are under increased monitoring by the FATF, but which are not included in Annex 4 (see List A). When assessing the country risk, the persons subject to due diligence must adequately take into account the situation in these countries or of persons from these countries. The respective country situation is described in the FATF statement "Jurisdictions under Increased Monitoring" linked above
- Global Terrorism Index (GTI) (countries with very high and high risk)

The FMA provides the persons subject to due diligence with a **list** of states which **consolidates** the above-mentioned publications. This list is updated when warranted:

List A (higher geographical risks according to Annex 2 Section A(c) SPG)

Following guideline 2.14 of the ML/TF Risk Factors Guidelines, the FMA assumes that the automatic exchange of information in tax matters (AEOI) significantly increases the transparency of entities and accounts and thus reduces the abuse potential for money laundering and terrorist financing to a certain extent. In the FMA's view, it can therefore be considered a risk-mitigating circumstance if all beneficial owners of a business relationship are disclosed within the framework of automatic exchange of information (AEOI) (this presupposes that the countries of residence concerned are AEOI partner jurisdictions). The persons subject to due diligence are free to decide whether they want to take this risk-reducing factor into account – risk-reducing factors may be taken into account, risk-increasing factors must be taken into account.

3.1.3 Products, services and transactions risk factors

When identifying the risk associated with their products, services or transactions, persons subject to due diligence must consider the risk related to:

1) the level of transparency or opaqueness the product, service or transaction affords;

2) the complexity of the product, service or transaction; and

3) the value or size of the product, service or transaction.

Risk factors persons subject to due diligence must consider when identifying the risk associated with a product, service or transaction's transparency include:

a) To what extent do products or services allow the customer or beneficial owner or distribution recipient structures to remain anonymous or facilitate hiding their identity? Potentially risky products and services include bearer shares, fiduciary deposits, shell companies, certain trusts and legal persons (such as foundations) that can be structured in such a way as to take advantage of anonymity.

b) To what extent is it possible for a third party that is not part of the business relationship to give instructions, for example in the case of certain correspondent banking relationships?

Factors that persons subject to due diligence must consider when identifying the risk associated with a product, service or transaction's complexity include:

a) How complex is the transaction and does it involve multiple parties or multiple countries, for example in the case of certain trade finance transactions? Are transactions straightforward, for example are regular payments made into a pension fund?

b) To what extent do products or services allow payments from third parties or accept overpayments where this is would not normally be expected? Where third party payments are expected, does the person subject to due diligence know the third party's identity, for example is it a state benefit authority or a guarantor? Or are products and services funded exclusively by fund transfers from the customer's own account at another financial institution that is subject to AML/CFT standards and oversight that are comparable to those required under the EU Anti-Money Laundering Directive?

c) Does the company understand the risks associated with its new or innovative product or service, in particular where this involves the use of new technologies or payment methods?

Factors that persons subject to due diligence must consider when identifying the risk associated with a product, service or transaction's value or size include:

a) To what extent are products or services cash intensive, as are many payment services but also certain current accounts?

b) To what extent do products or services facilitate or encourage high-value transactions? Are there any caps on transaction values or levels of premium that could limit the use of the product or service for ML/TF purposes?

3.1.4 Delivery channel risk factors

When identifying the risk associated with their delivery channels, persons subject to due diligence must consider the risk related to:

1) the extent to which the business relationship is conducted on a non-face-to-face basis; and

2) any introducers or intermediaries the firm might use and the nature of their relationship with the company.

When assessing the risk associated with the way in which the customer obtains the products or services, persons subject to due diligence must consider a number of factors including:

a) whether the customer is physically present for identification purposes. If they are not, whether the person subject to due diligence

- used a reliable form of non-face-to-face client identification (customer due diligence; CDD); and

- took steps to prevent impersonation or identity fraud.

b) whether the customer has been introduced by company subject to due diligence within the same financial group and, if so, to what extent the person subject to due diligence can rely on this introduction as reassurance that the customer will not expose the person subject to due diligence to excessive ML/TF risk, and what the company has done to satisfy itself that the other company subject to due diligence within the financial group applies measures according to the standards of the European Economic Area (EEA) that are also in line with the EU Anti-Money Laundering Directive when performing due diligence?

c) whether the customer has been introduced by a third party, for example a bank that is not part of the same group or an intermediary, and if so:

- whether the third party is a regulated person subject to AML obligations that are consistent with those of the EU Anti-Money Laundering Directive, and whether the third party is a financial institution or its main business activity is unrelated to financial service provision (see Annex 1 of FMA Instruction 2018/7).
- whether the third party applies due diligence measures, keeps records to EEA standards, is supervised for compliance with comparable AML/CFT obligations in line with Article 26 of Directive (EU) 2015/849, and whether there are any indications that the third party's quality of compliance with applicable AML/CFT legislation or regulation is inadequate, for example whether the third party has been sanctioned for breaches of AML/CFT obligations.
- whether the third party is based in a country associated with higher ML/TF risk (increased corruption risks and other predicate offences to money laundering must be considered here in particular).
- where a third party is based in a state with strategic deficiencies (Annex 4 SPV), persons subject to due diligence must not rely on that third party. Reliance on such intermediaries is possible only if the intermediary is a branch or majority-owned subsidiary of another company established in the Union, and the person subject to due diligence is confident that the intermediary fully complies with group-wide policies and procedures in line with Article 45 of EU Anti-Money Laundering Directive (EU) 2015/849.
- what the person subject to due diligence has done to satisfy itself that:
  - the third party always provides the necessary identity documentation.
  - the third party will provide, immediately upon request, relevant copies of identification and verification data or electronic data referred to in the SPG and the SPV.
  - the quality of the third party's due diligence measures is such that it can be relied upon; and
  - the level of due diligence applied by the third party is commensurate to the ML/TF risk associated with the business relationship, considering that the third party will have applied due diligence measures for its own purposes and, potentially, in a different context.

d) whether the customer has been introduced through a tied agent, that is, without direct contact to the company subject to due diligence, and to what extent the person subject to due diligence can be satisfied that the agent has obtained enough information to ensure that the company knows its customer and the level of risk associated with the business relationship;

e) whether independent or tied agents are used, to what extent they are involved on an ongoing basis in the conduct of business, and how this affects the company's knowledge of the customer and ongoing risk management;

f) when the company uses an outsourced service provider for aspects of its AML/CFT obligations, whether it has considered whether the outsourced service provider is a person or company subject to

due diligence, and whether it has addressed the risks set out in the EBA's Guidelines on outsourcing (EBA/GL/2019/02), where those guidelines are applicable.

3.2 Risk factors according to sector-specific guidelines

Please refer to the additional sector-specific risk factors under Title II of the ML/TF Risk Factors Guidelines.

Guideline 8	Sectoral guideline for correspondent relationships
Guideline 9	Sectoral guideline for retail banks
Guideline 10	Sectoral guideline for electronic money issuers
Guideline 11	Sectoral guideline for money remitters
Guideline 12	Sectoral guideline for wealth management
Guideline 13	Sectoral guideline for trade finance providers
Guideline 14	Sectoral guideline for life insurance undertakings
Guideline 15	Sectoral guideline for investment firms
Guideline 16	Sectoral guideline for providers of investment funds
Guideline 17	Sectoral guideline for regulated crowdfunding platforms
Guideline 18	Sectoral guideline for payment initiation service providers (PISPs) and account information service providers (AISPs)
Guideline 19	Sectoral guideline for firms providing activities of currency exchange offices
Guideline 20	Sectoral guideline for corporate finance

Liechtenstein persons subject to due diligence who offer products and services in the area of international wealth management (this also includes service providers for legal entities) must in particular also observe the factors listed in sectoral guideline 12 for wealth management.

In addition to the relevant factors set out in Annex 2 Section A SPG such as:

- legal entities that are personal asset-holding vehicles;
- companies that have nominee shareholders or shares in bearer form;
- cash-intensive businesses;
- given the nature of the company's business, the ownership structure of the company appears unusual or excessively complex;
- high value assets or high amount of transactions executed;
- banks offering private banking services;
- products or transactions that might favour anonymity;
- states with high geographical risks; etc.

sectoral guideline 12 lists the following risk-increasing factors:

- customers requesting large amounts of cash or other physical stores of value such as precious metals;
- very high-value transactions;

- financial arrangements involving countries associated with higher ML/TF risk (companies should pay particular attention to countries that have a culture of banking secrecy or that do not comply with international tax transparency standards);
- lending (including mortgages) secured against the value of assets in other countries, particularly countries where it is difficult to ascertain whether the customer has legitimate title to the collateral, or where the identities of parties guaranteeing the loan are hard to verify;
- the use of complex business structures such as trusts and private investment vehicles, particularly where the identity of the ultimate beneficial owner may be unclear;
- business taking place across multiple countries, particularly where it involves multiple providers of financial services;
- cross-border arrangements where assets are deposited or managed in another financial institution, either of the same financial group or outside the group, particularly where the other financial institution is based in a country associated with higher ML/TF risk. Persons subject to due diligence should pay particular attention to countries with higher levels of predicate offences, a weak AML/CFT regime or weak tax transparency standards.

3.3 Risks arising from the use of new technologies

Persons subject to due diligence must assess the use of new technologies for new or existing products or services or delivery channels and take appropriate measures to reduce the risk (Annex 2(A)(b)(5) SPG). New technologies may be introduced, for example, in connection with new asset classes, new delivery channels, or new payment methods. The assessment of the risks and the implementation of the measures must take place before the new technology is used. In addition, the risk assessment must be carried out either ad hoc or at the latest during the next scheduled update of the business risk assessment (after approval of the product introduction process with the inclusion of compliance). By way of clarification, the relevant risk factors must already be taken into account in the customer risk assessment when new technologies are used.

3.4 Other special risk factors for TT service providers

As a fundamental matter, the same risk factors exist for TT service providers as for equivalent services in the traditional financial sector. Beyond that, there are other specific risk factors to consider in the TT services sector that may contribute to an increase (or decrease) in risk.

Transaction-related risk factors:

- High exposure of the assets brought in to criminal activities, e.g. nexus to darknet market, ransomware, scams, or ICO fraud;
- Tokens or virtual currencies routed via peer-to-peer platforms;
- Tokens or virtual currencies whose transfer makes use of mixing or tumbling services;
- Transactions from and to unhosted wallets;
- Transactions for which the travel rule requirements under Article 12a SPG in conjunction with Articles 23d et seq. SPV were not met by the counterparty;
- Off-chain transactions;
- Inflows of tokens or virtual currencies from cryptocurrency ATMs;
- Transactions whose counterparty is a TT service provider with unknown domicile;
- Transactions whose counterparty is a TT service provider domiciled in a poorly regulated third country (e.g. countries with strategic deficiencies as referred to in Annex 4 SPV or the Seychelles[2]).

[2] https://ciphertrace.com/2020-geo-risk-report-on-vasp-kyc/

Customer-related risk factors:

- TT services for unregulated token issuers;
- Persons who become customers of the TT service provider without an identifiable background and from regions that are not actively solicited.

The following factors can have a risk-mitigating effect in relation to the customer:

- Whitelisting of the recipient addresses for token issues;
- Limited geographical exposure of the contracting party and the beneficial owners with a focus on the Germany, Austria, Switzerland, and Liechtenstein region.

Risk factors related to products and services:

- Use of anonymity-enhancing TT systems (privacy coins);
- TT services provided for clients by third-party TT service providers;
- TT services for third-party TT service providers which they need to offer TT services to their clients (liquidity creation, etc.);
- Exchange transactions in connection with an unregulated ICO.

In this context, the processing of TT services in a closed TT system with a centralised service provider can serve as a risk-reducing factor.

Risk factors related to terrorist financing:

- Nexus to countries with very high or high risk according to the Global Terrorism Index (GTI)[3] or according to FATF (e.g. Iran);
- Nexus of transactions countries with very high or high risk according to GTI or according to FATF (e.g. Iran);
- Frequent switching of assets to different TT systems;
- Transfers within related accounts/wallets for no apparent reason.

Risk factors related to new technologies:

- New business models, especially those that are decentralised, such as products in decentralised finance (DeFi).

3.5 Risk factors according to national risk assessments

According to Article 9a(2) SPG, the results of the national risk assessment pursuant to Article 29b SPG must also be taken into account. The FMA refers to the threats and risk factors identified in the following risk assessments:

- National Risk Assessment on Money Laundering II

- National Risk Assessment on Terrorist Financing

- National Risk Assessment on Virtual Asset Service Providers

[3] https://www.visionofhumanity.org/wp-content/uploads/2020/11/GTI-2020-web-1.pdf

4. Assessing ML/TF risk

Persons subject to due diligence must use the risk factors they have identified to assess the overall level of ML/TF risk.

4.1 Taking a holistic view

Persons subject to due diligence must take a holistic view of the ML/TF risk factors they have identified that, together, will determine the level of ML/TF risk associated with a business relationship, an occasional transaction, or their business.

With the exception of cases defined by law, the presence of isolated risk factors does not necessarily move a relationship into a higher or lower risk category.

4.2 Weighting risk factors

When assessing ML/TF risk, persons subject to due diligence may decide to weight factors differently depending on their relative importance.

When weighting risk factors, persons subject to due diligence should make an informed judgement about the relevance of different risk factors in the context of a business relationship, an occasional transaction or their business. This often results in persons subject to due diligence allocating different scores to different factors; for example, persons subject to due diligence may decide that a customer's personal links to a jurisdiction associated with higher ML/TF risk is less relevant in light of the features of the product they seek.

Ultimately, the weight given to each of these factors is likely to vary from product to product and customer to customer (or category of customer) and from one person subject to due diligence to another.

When weighting risk factors, persons subject to due diligence should ensure that:

a) weighting is not unduly influenced by just one factor;

b) economic or profit considerations do not influence the risk rating;

c) weighting does not lead to a situation where it is impossible for any business relationship to be classified as high risk;

d) weighting does not entail that business relationships or transactions defined as high risk by law are not ultimately classified as anything other than high risk in the overall consideration; and

e) the persons subject to due diligence may over-ride automatically generated risk scores only on important grounds. The rationale for the decision to over-ride an automatically generated result must be documented appropriately.

Where a person subject to due diligence uses automated IT systems to allocate overall risk scores to categorise business relationships or occasional transactions and does not develop these in house but purchases them from an external provider or uses a system developed by a supervisory authority or other institution, it should understand how the system works and how it combines or weights risk factors to achieve an overall risk score. A person subject to due diligence must always be able to satisfy itself that the scores allocated reflect its understanding of ML/TF risk and it should be able to demonstrate this to the competent authority.

4.3 Categorising risk

So that customer risk assessment can be applied in practice, the persons subject to due diligence must allocate the individual business relationships and transactions to the identified risks (see Article 9a(4) SPG). This allocation must be carried out by means of a risk categorisation system (e.g. "Risk Tool"). Only through

such a categorisation and allocation or labelling of the business relationships can the responsible employees subsequently correctly apply the measures envisaged for the individual risk categories.

The number of categories is defined by the persons subject to due diligence. The more risk categories are defined, the better the individual measures can be tailored to the respective risks. There cannot be a category with "zero risk". In this context, the FMA generally recommends a choice of four categories:

- Low risks (simplified due diligence, Article 10 SPG)
- Normal risks (regular due diligence)
- Higher risks (enhanced due diligence, Article 11(1) SPG, individual risks)
- High risks (enhanced due diligence, Article 11(4) to (6) and Article 11a SPG, automatic cases of enhanced due diligence)

It is up to the individual persons subject to due diligence to further expand or narrow down the 4-level categorisation proposed by the FMA, depending on the type of person subject to due diligence and the scope of its business activity (e.g. higher and high risks may be combined in a single category).

The categorisation must be documented in a comprehensible way and implemented in practice.

The allocation of individual transactions is relevant for those persons subject to due diligence who, in addition to long-term business relationships, also carry out occasional transactions (business and transactions carried out for one-off customers) as well as for those persons subject to due diligence for whom the establishment of a business relationship represents the exceptional case (e.g. traders in goods, agents of payment service providers, etc.).

In the business risk assessment, the inherent risks, the quality of mitigation measures, and the residual risk must be categorised appropriately. According to Article 9a(5) SPG, the persons subject to due diligence must subsequently define effective internal control and monitoring measures to reduce the risks identified in the national risk assessment and the business risk assessment.

In the case of risk factors for which high residual risks have been identified, it must be examined whether these risks indicate weaknesses in the defence mechanism, so that measures to reduce these risks must be defined. To do so, (a) the inherent risks can be targeted by reducing the exposure of the person subject to due diligence (de-risking) and/or (b) the measures for risk mitigation can be targeted by improving them (in this regard, the strengthening of personnel compliance resources should also be considered).

The internal control and monitoring measures must in particular take into account the following points:

- the implementation of due diligence pursuant to Article 5(1) SPG;
- documentation pursuant to Article 20 SPG;
- the design of the internal organisation and internal instructions pursuant to Article 21 SPG (written definition of responsibilities and service instructions, work aids (such as checklists, customer onboarding processes, forms, and the like));
- allocation of appropriate (sufficient) personnel resources and powers to the due diligence officer or compliance unit (second line of defence, e.g. mandatory involvement of the compliance unit when a business relationship with increased and high risk is established);
- allocation of appropriate (sufficient) personnel resources and powers to the investigating officer (third line of defence);
- collection of necessary data including involvement of other departments as well as assurance of data quality (also with regard to the level of detail of the data);
- regular employee training and awareness-raising regarding possible risk situations;

- use of IT systems for the prevention of money laundering and terrorist financing;
- performance of inspections incl. written record as part of a control plan; and
- documentation of results of measures performed.

5. Due diligence obligations

The business and company risk assessments conducted by a person subject to due diligence should help to identify where the person subject to due diligence should focus its ML/TF risk management efforts both when onboarding the client and for the duration of the business relationship as well as when carrying out occasional transactions.

Persons subject to due diligence must ensure that their AML/CFT policies and procedures build on and reflect their risk assessment.

They must also ensure that their AML/CFT policies and procedures are available to all relevant employees, are applied, and are effective and understandable.

According to Article 31(3) SPV, the instructions are to be issued at executive level. The persons subject to due diligence must therefore ensure that the executive level has access to sufficient data, including the business risk assessment, to gain a sound overview of the adequacy and effectiveness of these instructions and, in particular, of their due diligence measures and corresponding procedures.

The persons subject to due diligence must in principle apply all the due diligence measures defined in Article 5 SPG, but they may determine the scope of each of these measures on a risk-sensitive basis. The due diligence obligations are specified in more detail in FMA Instruction 2018/7.

The following sections refer only to simplified and enhanced due diligence.

5.1 Simplified due diligence

(Article 10 in conjunction with Annex 1 SPG, Articles 18(2) and 22b SPV)

Simplified due diligence obligations may be applied only if the persons subject to due diligence have identified a low risk of money laundering, organised crime, and terrorist financing in their risk assessment and have ensured that the business relationship or transaction concerned is indeed associated with a low risk. For the sake of completeness, please note that the application of simplified due diligence is excluded if there is a suspicion of money laundering, a predicate offence to money laundering, organised crime, or terrorist financing or if there are factors and possible indications of a potentially higher risk (see Article 22b(6) SPV). Pursuant to Article 27(1)(c^{bis}) SPV, application of simplified due diligence must be documented in the due diligence files or in other suitable internal documents (risk matrix or list of mandates).

Annex 1 of the Due Diligence Act contains factors and possible indicators of a potentially lower risk. On a supplemental basis, the risk factors referred to in Section 3 of this Guideline must be taken into account.

At this point it should be noted that even in the area of simplified due diligence, all due diligence obligations under Article 5(1)(a) to (d) SPG must be fulfilled. Only their scope or timing may vary, depending on the risk in question. The application of simplified due diligence is therefore no exception to the fulfilment of due diligence obligations.

With regard to the specific structuring of simplified due diligence in light of risk-appropriate monitoring, it is essential that simplified due diligence be structured at least in such a way that the persons subject to due diligence are in a position to identify unusual or suspicious transactions in order to be able to issue a suspicious transaction report if necessary.

As already explained, the persons subject to due diligence must in each individual case ensure that there is actually a low risk. Consequently, in cases of high and higher risks (legally as well as individually defined cases), the application of simplified due diligence is ruled out *per se*.

With regard to simplified due diligence relating to units of undertakings for collective investment (funds) as referred to in Article 22b(3) SPV, please refer to the explanations in FMA Instruction 2018/7.

5.2 Enhanced due diligence

(Article 2(1)(h), Article 11, Article 11a, and Annex 2 SPG in conjunction with Articles 2 and 23 SPV)

In cases of enhanced due diligence provided for by law (Article 11(4) to (6) and Article 11a(1) SPG), there is no discretion with regard to the application of enhanced due diligence. There is a certain leeway only with regard to the type and scope of the measures to be applied, provided that certain measures are not already mandatory by law (e.g. Article 11(4) and (4a) SPG in the case of PEPs).

Enhanced due diligence obligations must be applied in addition to the regular due diligence obligations and must in any case have an intensifying effect on the scope of the measures to be applied.

In addition to the cases defined by law, enhanced due diligence must also be applied if the person subject to due diligence has identified a higher risk of money laundering, organised crime, or terrorist financing on the basis of the risk assessment pursuant to Article 9a(4) SPG (see Article 11(1) SPG). In addition to the due diligence obligations set out in Articles 5 to 9 SPG, enhanced due diligence within the meaning of Annex 2 Section B SPG must be applied to the business relationships and transactions identified within the framework of the risk assessment in order to adequately manage and mitigate the higher risks.

With regard to specific measures, those in Annex 2 Section B of the Due Diligence Act and the ML/TF Risk Factors Guidelines (see guideline 4.62) must be taken into account. However, persons subject to due diligence are free to lay down further effective enhanced measures in their risk assessment or internal instructions.

Pursuant to Article 27(1)(c^{bis}) SPV, application of enhanced due diligence must be documented in the due diligence files or in other suitable internal documents (risk matrix or list of mandates).

5.2.1 Politically exposed persons (PEPs)

(Article 2(1)(h) in conjunction with Article 11(4) and (4a) SPG in conjunction with Articles 2, 21, and 23 SPV)

In business relationships with PEPs, persons subject to due diligence must apply the enhanced due diligence obligations defined in Article 11(4) SPG (see also FMA Instruction 2018/7).

In the case of domestic PEPs,[4] persons subject to due diligence may refrain from applying enhanced due diligence if lower risks have been identified, once a risk assessment has been conducted (see FATF Guidance Politically Exposed Persons, 26 et seq.[5]).

This risk assessment must take into account all relevant risk factors in order to determine whether or not enhanced due diligence must be applied with respect to the particular business relationship with a domestic PEP. In particular, the persons subject to due diligence must obtain sufficient information to understand the particular characteristics of the prominent domestic public functions. The risk assessment must also take into account factors relating to customer risk, geographical risk and product, service, transaction, or delivery channel risk (see Annex 2 Section B SPG). In addition, the nature of the prominent public functions, such as level of seniority, access to or control over public funds, and the nature of the position held, must be taken into account.

[4] i.e. persons with prominent public functions in Liechtenstein as well as immediate family members and known close associates

[5] https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf

If the person subject to due diligence comes to the conclusion through the risk assessment that no higher risks emanate from the business relationship with the domestic PEP, no enhanced due diligence has to be applied. If the risk assessment suggests a higher risk, enhanced due diligence obligations and measures must be applied, analogous to business relationships with foreign PEPs.

Details of the expectations in connection with the necessary PEP checks are addressed in the FMA's sector-specific guidelines in FMA Instruction 2018/7.

It should be noted here that a business relationship is to be qualified as a PEP business relationship, irrespective of whether the contracting party and/or the beneficial owner and/or the recipient of a distribution is a PEP (the term "PEP" also includes immediate family members or persons who are known to be close associates).

In addition, holders of important offices in international governmental organisations (e.g. the European Union, the United Nations, NATO, etc.) are now also subsumed under the term "PEP" (see Article 2(1)(g) SPV).

In principle, even a one-time distribution to a PEP results in a business relationship being classified on a mandatory basis as a PEP business relationship within the meaning of Article 11(4) SPG for one year after the recipient of a distribution has held public office. But if no further distributions are made to this PEP, the FMA assumes a comparatively lower risk than in the case of business relationships in which the settlor/founder is qualified as a PEP. In this context, yearly approval by a member of the executive body pursuant to Article 11(4)(c) SPG may be waived in the case of a one-time distribution to a PEP. In addition, there is leeway as part of enhanced continuous monitoring, for instance by establishing higher thresholds compared with business relationships in which the settlor/founder is qualified as a PEP.

If higher risks have been identified in a life insurance company or another insurance with an investment purpose, the persons subject to due diligence (primarily insurance undertakings) must, in addition to the measures pursuant to Article 11(4a)(a) and (b) SPG, examine whether a report must be submitted to the FIU under Article 17 SPG. This obligation to examine whether a report must be submitted to the FIU pursuant to Article 17 SPG applies in principle to all persons subject to due diligence.

5.2.1.1 Former PEP

With regard to the qualification of the contracting party or the beneficial owner as a former PEP, the person subject to due diligence must individually check after expiry of the one-year period under Article 2(1)(h) SPG whether there is still a high risk.

It should be noted in this regard that the risk arising from a PEP does not drop abruptly when the function comes to an end. For this reason, a careful examination of each individual case is necessary in order to be able to make a risk-appropriate decision. A decision to assign the business relationship to a lower risk category must be justified and documented.

Depending on the individual risk categorisation, enhanced due diligence must then continue to apply in accordance with Article 11(1) SPG. If the person subject to due diligence concludes that the former PEP no longer represents a higher risk one year after the end of the PEP's term of office, immediate family members and persons who are known to be close associates are no longer classified as higher risk. This decision must be documented accordingly.

5.2.2 Correspondent banking relationships

(Articles 11(5) and 16 SPG in conjunction with Article 16 SPV)

According to Article 11(1) in conjunction with Article 11(5) SPG, it must always be assumed in cases of cross-border correspondent banking relationships with respondent institutions in a third country that business relationships and transactions have higher risks. Therefore, in addition to the regular due diligence obligations, at least the measures specified in Article 11(5)(a) to (d) SPG must be taken.

However, due to the requirements set out in Article 16 SPG ("strategies and procedures applying throughout the group for the prevention of money laundering, organised crime, and the terrorist financing") that already have to be fulfilled, the FMA is of the opinion that intragroup correspondent banking relationships in third countries cannot be assumed to have the same risk as correspondent banking relationships in third countries outside the group.

In the case of intragroup correspondent banking relationships, the strategies and procedures provided for in Article 16 SPG must already be effectively implemented at the level of branches, agents, representative offices, and subsidiaries in EEA Member States and third countries that are majority owned by the persons subject to due diligence. This means that the higher risks associated by their nature with correspondent banking relationships are in principle already addressed in a risk-appropriate manner, so that in the FMA's view no additional measures are required. Insofar as the measures required by Article 16 SPG cannot be complied with, Article 16(3) SPG already sets out a duty of the person subject to due diligence to act and to provide information to the FMA.

The FMA's expectation in cases of intragroup correspondent banking relationships in third countries is therefore limited to compliance with the provisions of Article 16 SPG and regular inspections of compliance with those provisions in order to meet the requirement of enhanced due diligence. It is therefore decisive in individual cases whether the respondent institution is covered by the definition of "group" referred to in Article 16 SPG. More far-reaching measures may, however, be required in individual cases based on additional risk factors of the business relationship, even in the case of intragroup correspondent banking relationships in third countries.

If the intragroup respondent institution is located in a state with strategic deficiencies as defined in Article 2(1)(u) SPG, further additional measures must always be applied.

Furthermore, risk categorisation must continue to be carried out as "higher risk", even in the case of intragroup correspondent banking relationships.

5.2.3 Complex structures and transactions

(Article 11(6) SPG)

According to Article 11(6) SPG, enhanced monitoring must be applied to complex structures, complex and unusually large transactions, as well as transaction patterns that have no apparent financial purpose or discernible lawful purpose and, to the extent possible, their background and purpose must be investigated and the results recorded in writing.

The determination of whether a structure is complex or whether a transaction is complex and unusually large depends on the underlying criteria. The assessment must therefore be carried out by the person subject to due diligence, based on the relevant criteria that the person subject to due diligence defines internally. In all cases, the assessment must be adequately documented in combination with the criteria relevant for the assessment.

Essentially, structures and transactions must be recorded if their complexity impairs transparency (from the perspective of the person subject to due diligence) with regard to information relevant under due diligence law. For example, the following criteria may be important for assessing complexity:

- number of underlying companies included in the structure;
- number of countries involved and their geographical risk;
- economic reasonableness of the structure;
- extent to which information on the structure relevant to due diligence law is available in official registers or publicly certified documents.

Various risk-increasing and risk-reducing factors also play a role in the risk assessment.

For example, the following criteria may be **risk-reducing**:

- the person subject to due diligence was involved in the establishment of the structure;
- the person subject to due diligence serves in a governing body of the structure;
- many years of experience of the person subject to due diligence in relation to a particular form of structuring;
- long-standing business relationship with frequent client contact;
- branch establishment or representative office in the countries involved ("country desks") or correspondingly extensive experience (knowledge of the language as well as political, sociocultural, and regulatory background knowledge) with regard to the countries involved.
- involvement of EEA/EU/equivalent third countries.

The following **risk-increasing** factors must be taken into account in particular:

- individual signatory powers and general/special powers of attorney of external third parties;
- structures established by third parties;
- involvement of countries with which the person subject to due diligence has no experience;
- involvement of third countries that are not considered to be equivalent;
- recently established business relationship;
- rare client contacts;
- unclear purpose or economically questionable structuring at the client's request;
- deviation from the previously known needs of the client (see business profile), i.e. atypical and incomprehensible structuring;
- type of transaction (e.g. OTC derivatives transaction or a letter of credit transaction).

It should be noted in this regard that the existence of a single criterion is generally not sufficient to judge the complexity of a business relationship or transaction – the overall view, taking into account all relevant criteria, is decisive.

5.2.4 States with strategic deficiencies

(Articles 2(1)(u) and 11a SPG in conjunction with Art. 23a and Annex 4 SPV)

According to Article 11a SPG, persons subject to due diligence must apply enhanced due diligence as set out in Annex 2 Section B SPG in relation to business relationships and transactions involving states with strategic deficiencies (Article 2(1)(u) SPG, Article 23a SPV in conjunction with Annex 4 SPV).

States with strategic deficiencies are those whose national systems for the prevention of money laundering and terrorist financing pursuant to Commission Delegated Regulation (EU) 2016/1675 or according to the assessments of international bodies (especially FATF, Moneyval, etc.) exhibit strategic deficiencies relating to AML/CFT and accordingly pose significant threats to the financial system (see Article 2(1)(u) SPG).

If the countries listed in Annex 4 SPV are involved in business relationships or transactions, enhanced due diligence is therefore triggered in all cases – i.e. irrespective of whether further risk factors are present – and the additional measures listed in Annex 2 Section B SPG must necessarily be applied.

Following the requirements set out in the ML/TF Risk Factors Guidelines (guidelines 4.53 et seq.), the following points specify how such involvement arises. Accordingly, a business relationship or occasional transaction must always be deemed to involve a state with strategic deficiencies (hereinafter also: "high-risk third country") if:

1. the funds were generated in a high-risk third country;
2. the funds are received from a high-risk third country;
3. the destination of funds is a high-risk third country (domicile of the payment service provider);
4. the person subject to due diligence is dealing with a natural person or legal person resident or established in a high-risk third country;
5. the person subject to due diligence is dealing with a trustee or trust that is resident or established in a high-risk third country or with a trust governed under the law of a high-risk third country.

The ML/TF Risk Factors Guidelines also require that enhanced due diligence (as set out in Annex 2 Section B SPG) be performed in the context of a business relationship if:

1. the transaction passes through a high-risk third country, for example because of where the intermediary payment services provider is based;
2. a beneficial owner in the business relationship is resident in a high-risk third country.

Irrespective of the criteria above, persons subject to due diligence must also carefully assess the risk associated with business relationships and transactions where:

1. the customer is known to maintain close personal or professional links with a high-risk third country, or
2. beneficial owner(s) is/are known to maintain close personal or professional links with a high-risk third country.

In those situations, persons subject to due diligence must take a risk-based decision on whether or not to apply enhanced due diligence (as set out in Annex 2 Section B SPG).

If a transaction is carried out within the framework of a business relationship that has a link to a state with strategic deficiencies, the entire business relationship must in principle be monitored more closely.

We also refer to the explanations in Report and Motion No. 48/2020, according to which any nexus with a states with strategic deficiencies must be examined on the basis of the information that the persons subject to due diligence already have or must have pursuant to other SPG obligations (in particular business profile, transaction clarification) or pursuant to the Funds Transfer Regulation (information on the payer and payee). Article 11a SPG is not intended to establish a blanket additional duty of verification or clarification that goes beyond that information.

6. Annexes

6.1 Annex 1 – Guidance for business risk assessment

The individual steps of a business risk assessment are outlined below. Alternative approaches to risk assessment can also be chosen, but the steps of a risk assessment outlined below should essentially also be reflected in alternative approaches.

6.1.1 Step 1: Taking stock

At the beginning of a risk assessment, comprehensive stocktaking of the institution-specific situation is required.

This includes general company key figures, business strategy (e.g. business policy and areas), business environment, and target markets as well as the AML organisation. This stocktaking must be documented.

For this introductory stocktaking, the data reported to the FMA in the electronic reporting form for risk assessment under the SPG (SPG report) should in particular also be taken into account.

By way of example, the following points should be addressed when taking stock:

- How is the institution organised (head office, balance sheet total, assets under management, employees, management board, supervisory board, significant participations, etc.)?
- What areas are outsourced?
- What are the business environment and target market (e.g. regional profile, profile of potential customers)?
- Have there been any significant changes in the customer structure or in the products, services, or delivery channels in recent years? Change in business strategy?
- How are the business policies and areas set up (core business, etc.)?
- What delivery channels exist (e.g. via qualified third parties or intermediaries)?
- To what extent are new technologies used (for example in connection with customer identification)?

6.1.2 Step 2: Identification of all relevant risk factors

In a second step, the person subject to due diligence must define which risk factors are relevant with regard to the concrete company-specific situation and the business strategy. In particular, the national risk assessments, the risk factors in the Annex to the SPG, and the factors in FMA Guideline 2013/1 and in the ML/TF Risk Factors Guidelines (EBA/GL/2021/02) must be taken into account. The persons subject to due diligence must at least take into account factors relating to customer risks, geographical risks, product and service risks, transaction risks, and delivery channel risks.

6.1.3 Step 3: Abstract assessment of the risk factors identified (= abstract inherent risk)

In a third step, the risk factors identified by the person subject to due diligence are analysed and the inherent risk of the individual factors is assessed in the abstract, i.e. independently of the specific exposure of the person subject to due diligence. For example, domestic PEPs pose a lower inherent risk in the abstract than foreign PEPs: Experience shows that any money related to corruption tends to be placed outside the home country. Another example: Clients from countries with lower levels of corruption typically pose lower inherent money laundering risks than clients from countries with high levels of corruption.

6.1.4 Step 4: Assessment of exposure based on company-specific key figures

In a fourth step, the risk factors that have been identified and then assessed in the abstract are assessed on the basis of company-specific key figures. For example, an exposure with regard to foreign PEPs can be assumed if the person subject to due diligence already has numerous foreign PEPs as clients or if business acquisition focuses on target markets (countries with higher corruption risks) and/or client segments (wealth management) that entail a high probability of knowing or unknowing acquisition of PEPs, including immediate family members or known close associates.

Another example: A person subject to due diligence which, according to internal guidelines, does not permit business relationships with entities with bearer shares and in fact ensures compliance with these guidelines has a low exposure to the risk factor "legal entities with bearer shares".

6.1.5 Step 5: Assessment of inherent risk taking into account the exposure

Taking into account the exposure determined in the fourth step, the inherent risk for the specific institution must then be assessed.

6.1.6 Step 6: Analysis of risk-mitigating measures for each of the inherent risks

In a sixth step, the measures implemented by the person subject to due diligence to mitigate the inherent risks must be analysed and documented for each risk factor. The focus should be on the measures that serve specifically to mitigate that risk factor.

For instance, in the case of the PEP risk factor, the person subject to due diligence must analyse and document whether an effective PEP screening tool is in use, and to what extent and with what frequency the client base is subjected to PEP screening. Furthermore, it must be checked whether sufficient and suitable (and trained) personnel resources are available to process the potential hits from the PEP screening (including any language skills that may be required). Also of importance are the standards implemented in the determination and plausibility check of the total assets and the contributed assets of PEPs, etc.

6.1.7 Step 7: Assessment of the risk-mitigating measures

The measures analysed in the sixth step are to be evaluated in a next step with regard to their effectiveness. For example, information, findings, etc. on the part of the compliance unit, the investigating officer, the internal audit, or findings in the context of inspection activities by the FMA or mandated auditors must also be taken into account.

6.1.8 Step 8: Assessment/derivation of residual risk

In an eighth step, the residual risk is derived on the basis of the individual results. The remaining residual risk must be derived at (a) the level of the individual risk factors, (b) the level of the risk categories (geographical risk, customer risk, etc.), and (c) the overall level.

6.1.9 Step 9: Derivation of any measures

A good business risk assessment aims to show whether the risks with which the person subject to due diligence is confronted are adequately mitigated or whether there are areas that are not adequately addressed by risk management. In the case of risk factors for which high residual risks have been identified, it must be examined whether these risks indicate weaknesses in the defence mechanism, so that measures to reduce these risks must be defined. To do so, (a) the inherent risks can be targeted by reducing the exposure of the person subject to due diligence (de-risking) and/or (b) the measures for risk mitigation can be targeted by improving them (in this regard, the strengthening of personnel compliance resources should also be considered).

At least in the case of financial institutions (persons subject to due diligence as referred to in Article 3(1)(a) to (i) SPG), the FMA recommends a separate presentation of the overall risk for (a) money laundering, (b) terrorist financing, and (c) evasion of international sanctions (see last lines of the following template for business risk assessment).

6.1.10 Step 10: Risk appetite

The risk-appetite statement helps to specify the scope of risk that the company is prepared to take on within the framework of its risk-bearing capacity. The written statement provides information on the type and extent of risks deliberately taken on in order to achieve the business objectives. The company compares the results of the business risk assessment (BRA) and the resulting residual risk with the risk appetite defined for the company, i.e. it is checked whether the resulting residual risk is within the scope of the defined risk appetite or not.

FMA

Finanzmarktaufsicht
Liechtenstein

Template for business risk assessment

Step 1 Taking stock	Step 2	Step 3	Step 4	Step 5	Step 6	Step 7	Step 8	Step 9	Step 10
	Identification of all risk factors at company level (NRA, ML/TF Risk Factors Guidelines, etc.)	*Assessment of abstract inherent risk*	*Assessment of exposure of persons subject to due diligence (likelihood & impact)*	*Assessment of inherent risk due to exposure*	*Derivation of risk-mitigating measures*	*Assessment of risk-mitigating measures*	*Assessment of residual risk*	*Derivation of necessary measures*	*Risk appetite*
		very low – very high	*very low – very high*	*very low – very high*		*not effective – very effective*	*very low – very high*		*very low – very high*
Customer risk	*Risk factor*								
	Risk factor								
	etc.								
Sub-risk customers									
Geographical risks	*Risk factor*								
	Risk factor								
	etc.								
Sub-risk geography									
Product and service risks	*Risk factor*								
	Risk factor								
	etc.								
Sub-risk products and									
Transaction risks	*Risk factor*								
	Risk factor								
	etc.								
Sub-risk transactions									
Delivery channel risks	*Risk factor*								
	Risk factor								
	etc.								
Sub-risk delivery channel									
A) Total risk money laundering									
B) Total risk terrorist financing									
C) Risk of evasion of international									

Landstrasse 109 • Postfach 279 • 9490 Vaduz • Liechtenstein
Telefon +423 236 73 73 • Telefax +423 236 73 74 • www.fma-li.li • info@fma-li.li

6.2 Annex 2 – Examples of risk categorisation and risk weighting

By way of illustration, here are some examples reflecting the FMA's interpretation and minimum expectations with regard to risk categorisation and risk weighting under Article 9a(4) SPG in dealing with individual cases. In the example cases with higher risks, the FMA assumes that there are no factors which would permit a lower risk categorisation.

All examples relate to the specific circumstances described in each case and are based on the assumption that at the time of the risk assessment, there are no incidents, media reports (see also the comments above on media monitoring), or other indicators of a potentially higher risk for the respective business relationship that are relevant to risk categorisation.

Furthermore, the examples are valid only if there is no reason to apply enhanced due diligence in accordance with Article 11(4) to (6) SPG (PEPs, complex structures/transactions, CP/BO/recipient of a distribution in states with strategic deficiencies).

Example 1

- Retail or corporate client (natural or legal person[6])
- Work in the IT sector
- BOs are domiciled in countries where there is no higher geographical risk (see "Digression: Geographical factors)
- Low annual transaction volume

▶ The business relationship can be classified as a business relationship with low risks

Example 2

- Corporate client (natural or legal person[3])
- Large companies or SMEs with registered office in Liechtenstein, Switzerland, Austria
- BOs are domiciled in countries where there is no higher geographical risk (see "Digression: Geographical factors)
- High annual transaction volume

▶ The business relationship can be classified as a business relationship with normal risk

Example 3

- Wealth management client (natural person or legal entity[3] without a commercial business in the country of domicile)
- BOs are domiciled in countries where there is no higher geographical risk (see "Digression: Geographical factors)
- Low annual transaction volume

▶ The business relationship can be classified as a business relationship with normal risk

6 This includes the management of a legal entity as well as any other services for a legal entity that are subject to due diligence.

Example 4

- Wealth management client (natural person or legal entity[3] without a commercial business in the country of domicile)
- BOs are domiciled in countries with a higher geographical risk (see "Digression: Geographical factors").

▶ The business relationship must be classified as a business relationship with higher risks

Example 5

- Client is a natural person or a legal entity[3] without a commercial business in the country of domicile
- Client carries out import/export transactions (goods do not reach Liechtenstein; there is hardly any publicly available, independent information on the client's business partners)
- High annual transaction volume

▶ The business relationship must be classified as a business relationship with higher risks

Example 6

- The client of an asset manager is a natural person or legal entity
- The assets are posted to a bank account or custody account specific to the client which is held with a bank subject to due diligence
- BOs are domiciled in countries where there is no higher geographical risk (see "Digression: Geographical factors)
- Low annual transaction volume

▶ The business relationship can be classified as a business relationship with normal risk

Example 7

- It can be seen from the constituent documents of a Liechtenstein AIF that it serves as a vehicle for individual asset structuring
- BOs are domiciled in countries with higher geographical risk
- The initial subscription has a high volume

▶ The business relationship must be classified as a business relationship with higher risks

Example 8

- Client is an online borrower with a small loan amount
- BOs are domiciled in countries where there is no higher geographical risk (see "Digression: Geographical factors)

▶ The business relationship can be classified as a business relationship with low risks

Example 9

- Client is the owner of an occupational pension account and has no power to dispose of the account
- The account includes only saved assets

▶ The business relationship can be classified as a business relationship with low risks

6.3 Annex 3 – Business risk assessment and customer risk assessment tools

In cooperation with the individual sectors, the FMA has developed tools for the risk assessment of business relationships as required under this FMA Guideline ("CRA Tool"). These tools are available on request from the FMA.

The persons subject to due diligence must check whether the CRA tool is suitable for their specific situation and adapt it if necessary. When applying the CRA Tool for risk assessment, the requirements regarding risk assessment set out in the SPG/SPV and this Guideline are deemed to be met. The CRA Tool is intended to define a common minimum standard. Above all, the tool aims to provide legal certainty with regard to due diligence.

When persons subject to due diligence develop and use their own risk assessment systems, the expectation of the FMA is that these systems do not lead to a lower risk categorisation in the example cases referred to in Annex 2 of the present FMA Guideline.

Additionally, some business associations (e.g. Liechtenstein Institute of Professional Trustees and Fiduciaries, THK) in cooperation with the FMA have developed tools for the business risk assessment of business relationships as required under this FMA Guideline ("BRA Tool"). These tools are available upon request from the respective business association.

Here again, persons subject to due diligence must ensure that their business risk assessment is tailored to their business model and takes into account the factors and risks specific to the persons subject to due diligence.

The person subject to due diligence, of course, is free to undertake a more detailed risk assessment of their business relationships.

7. Entry into force

This Guideline was first adopted by the Board of Directors on 4 March 2013 and entered into force on the same day.

The amendments of 15 November 2017 (comprehensive revision) shall enter into force on the same day.

The changes of 26 March 2020 come into effect on 15 April 2020.

The changes of 23 July 2021 come into effect on 1 September 2021.

Status: 23 July 2021

8. Amendments

This Guideline was comprehensively revised on 15 November 2017.

The revised version addresses in particular the legislative changes in the area of due diligence that entered into force on 1 September 2017.

On 20 February 2018, the Guideline was supplemented by section 5.9 "Business Relationship Risk Assessment Tool for Service Providers for Legal Entities".

On 26 March 2020, the Guideline was expanded to include the following points:

- Section 4.2
  Addition of TT service provider

- Section 4.3.1.2
  Addition of risk factors related to TT services

- Section 4.4.1
  Inclusion of reference to Global Terrorism Index
  Deletion of the heading “List A”

- Section 4.4.2
  Deletion of the heading “List B”
  Designation of third countries whose systems for combating money laundering and terrorist financing work well or whose AML and CFT requirements, according to credible sources, are consistent with the FATF Recommendations 2012 and effectively implement these requirements.
  Deletion of paragraph List C (new addition will be made in guidance 2018/7)

- Section 5.3.3
  Recording of blockchain data

- Section 5.4.
  Expansion of the blockchain data management in stock and corresponding analysis tools.

- Standardisation of the terms "regular due diligence" and "normal risks"

On 23 July 2021, the following adjustments were made:

- New Chapter 1: General remarks

- New Chapter 2: Basic principles of risk assessment

- New Chapter 3: Identifying risk factors

- New Chapter 4: Assessing ML/TF risk

- Chapter 5: Due diligence obligations
  Deletion of previous Sections 5.1 to 5.4 (moved to FMA Instruction 2018/7)
  5.1. Simplified due diligence: Additional notes that the application of simplified due diligence is excluded in cases of suspicion covered by Article 17 SPG or if there are factors and possible indications of a potentially higher risk, and that explanations relating to units of undertakings for collective investment (funds) can be found in FMA Instruction 2018/7.
  5.2. Enhanced due diligence: More precise reference to Article 9a(4) SPG and reference to ML/TF Risk Factors Guidelines (instead of ESA Guidelines).

5.2.1. Politically exposed persons: Explicit mention of obligation to examine whether a report must be submitted to the FIU under Article 17 SPG, especially in the case of life insurance companies with higher risks.

5.2.1.1. Facilitations in performance of due diligence in regard to domestic PEPs.

5.2.2. Correspondent banking relationships: Adjustment to revised Article 11(5) SPG (LGBl. 2020 No. 305), according to which enhanced due diligence must also be applied to business relationships with respondent institutions in the EEA.

5.2.3. Complex structures and transactions: Adjustment of Article 11(6) SPG to the new legislative text and elimination of a risk-mitigating factor

5.2.4. States with strategic deficiencies: Adjustment to requirement in guidelines 4.53 et seq. of ML/TF Risk Factors Guidelines

- New Chapter 6: Annexes

  New Annex 1 – Guidance for business risk assessment

  Annex 2: Examples of risk categorisation and risk weighting (corresponds to previous Section 5.7 of the Guideline); Example 7: Addition of more meaningful fact pattern.

  Annex 3: Business risk assessment and customer risk assessment tools. Corresponds in principle to previous Section 5.9 of the Guideline, supplemented by the note that tools for carrying out the business risk assessment are now also available from the business associations.

- Deletion of Chapter 6 "More information on the risk-based approach": The link to the supranational risk assessment of the EU can now be found in Section 2.4.4.

- Deletion of Annex 9: The link to the ML/TF Risk Factors Guidelines and to simplified and enhanced due diligence can now be found under Section 1.2.