BANKA SLOVENIJE

EVROSISTEM

Pursuant to Article 31 of the Bank of Slovenia Act (Official Gazette of the Republic of Slovenia, Nos. 72/06 [official consolidated version], 59/11 and 55/17; hereinafter: the ZBS-1) and Article 169 of the Prevention of Money Laundering and Terrorist Financing Act (Official Gazette of the Republic of Slovenia, No. 48/22; hereinafter: the ZPPDFT-2), at its meeting of 5 May 2022 the Governing Board of Banka Slovenije adopted the following:

Guidelines on the assessment of the risk of money laundering and terrorist financing

Update 2022

List of abbreviations

AMLD	Directive (EU) 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and Directive (EU) 2018/843 of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU
AJPES	Agency of the Republic of Slovenia for Public Legal Records and Related Services
BCBS	Basel Committee on Banking Supervision
BoS	Banka Slovenije
BO	Beneficial owner
e-money	Electronic money (the same meaning as defined in the law governing payment services and systems)
EEA	European Economic Area
EU	European Union
EBA	European Banking Authority
FATF	Financial Action Task Force
FBE	Consolidated list of persons, groups and entities involved in terrorist acts to whom EU restrictive measures apply
TF	Terrorist financing
KDD	Central Securities Clearing Corporation
KYC	Know your customer
Moneyval	Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism, Council of Europe
National risk assessment	Report on the Republic of Slovenia's national risk assessment for money laundering and terrorist financing (current summary referenced 460-19/2019-130 was published in May 2021)
Supranational risk assessment	Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities (current report: COM/2019/370)
ML	Money laundering
PEP	Politically exposed person
AML/CFT officer	Officer for anti-money laundering and countering the financing of terrorism
AML/CFT	Anti-money laundering and countering the financing of terrorism
PRADO	Public Register of Authentic identity and travel Documents Online
ML/TF risk factors guidelines	Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions (EBA/GL/2021/02), which was issued on 1 March 2021 by the EBA
Guidelines	Guidelines on the assessment of the risk of money laundering and terrorist financing approved by the Governing Board of Banka Slovenije on 5 May 2022
Risk levels: LR, MR, IR, HR	In determining risk levels, the guidelines distinguish between low risk (LR), medium risk (MR), increased risk (IR) and high risk (HR)
FIU	FIU of the Republic of Slovenia for Money Laundering Prevention, Cankarjeva 5, 1000 Ljubljana

ZBS-1	Law governing Banka Slovenije in its currently applicable wording; on the day of issuance of the guidelines it was the Bank of Slovenia Act (Official Gazette of the Republic of Slovenia, Nos. 72/06 [official consolidated version], 59/11 and 55/17)
ZGD-1	Law governing commercial companies in its currently applicable wording; on the day of issuance of the guidelines it was the Companies Act (Official Gazette of the Republic of Slovenia, Nos. 65/09 [official consolidated version], 33/11, 91/11, 32/12, 57/12, 44/13 [constitutional court decision], 82/13, 55/15, 15/17, 22/19 [ZPosS], 158/20 [ZIntPK-C] and 18/21)
ZOUPAMO	Law governing restrictive measures in its currently applicable wording; on the day of issuance of the guidelines it was the Act Governing Restrictive Measures Introduced or Implemented by the Republic of Slovenia in Compliance with Legal Instruments and Decisions Adopted by International Organisations (Official Gazette of the Republic of Slovenia, Nos. 127/06 and 44/22)
ZPlaSSIED	Law governing payment services, electronic money issuance services and payment systems in its currently applicable wording; on the day of issuance of the guidelines it was the Payment Services, Electronic Money Issuance Services and Payment Systems Act (Official Gazette of the Republic of Slovenia, Nos. 7/18, 9/18 [corrigendum] and 102/20)
ZPPDFT-2	Law governing the prevention of money laundering and terrorist financing in its currently applicable wording; on the day of issuance of the guidelines it was the Prevention of Money Laundering and Terrorist Financing Act (Official Gazette of the Republic of Slovenia, No. 48/22)

1. Purpose, scope of application and definition of terms

1.1. Purpose

For the effective management of ML/TF risks, obliged entities are required under the **ZPPDFT-2** to identify and assess risks of this type, and on this basis to tailor their control environment to be commensurate with the assessed ML/TF risks.

In accordance with Article 169 of the ZPPDFT-2, Banka Slovenije is issuing these **guidelines**, by virtue of which it is issuing guidance with regard to the implementation of individual requirements of the ZPPDFT-2 relating to:

- the ML/TF risk assessment;
- the establishment and verification of customer's identity;
- the scope of customer due diligence;
- the procedures and measures for diligent monitoring of customers' business activities;
- customer acceptance policy;
- prohibited transactions; and
- sectoral guidelines for individual obliged entities.

In meeting the requirements obliged entities are also required to uphold the **ML/TF risk factors guidelines**, which were issued by the EBA in March 2021 on the basis of the AMLD, whose direct application to obliged entities referred to in Section 1.2 of the guidelines, with the exception of obliged entities referred to in point 6 of the aforementioned section, was set out by Banka Slovenije by virtue of the Regulation on the application of the Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions (Official Gazette of the Republic of Slovenia, No. 153/21).

For the effective management of ML/TF risks, obliged entities should draw up or update policies, procedures and controls in accordance with the ML/TF risk factors guidelines. Obliged entities are required to update policies, procedures and internal controls by the deadline defined in the final provisions (*see Section 7 Final provisions*). Where the ML/TF risk factors guidelines set out a different risk level or different measures, obliged entities should uphold the more stringent criteria or apply the measures cumulatively.

1.2. Scope of application

The guidelines are addressed to obliged entities for which Banka Slovenije is defined as a competent supervisory authority in accordance with the first paragraph of Article 164 of the ZPPDFT-2, namely:

1. banks, their branches in Member States, and branches of banks (of Member States and third countries) established in the Republic of Slovenia (hereinafter: **banks**);
2. **savings banks**;
3. payment institutions, payment institutions with a waiver, and payment institutions and payment institutions with a waiver of Member States that establish a branch in the Republic of Slovenia or provide payment services in the Republic of Slovenia via an agent (hereinafter: **payment institutions**);
4. electronic money institutions, electronic money institutions with a waiver, branches of third-country electronic money institutions and branches of Member-State electronic money institutions that establish a branch in the Republic of Slovenia or distribute and redeem e-money in the Republic of Slovenia on their own behalf via a distributor (hereinafter: **e-money issuers**);

5. **currency exchange offices**;
6. legal and natural persons during the pursuit of their business activities and professional activities in virtual currency services or other transactions included in such services (hereinafter: **virtual currency service providers**).

Having regard for the report on the findings of the national risk assessment and the supranational risk assessment, the guidelines contain "**general guidelines**" that apply to all obliged entities, except in the parts where "**sectoral guidelines**" set out special features and certain simplifications for individual categories of obliged entities in accordance with the principle of proportionality.

The set of risk criteria and measures cited in the guidelines is not exhaustive, and obliged entities therefore need to take appropriate account of other risk criteria and measures for the effective management of ML/TF risks as necessary.

The guidelines do not apply to restrictive measures, which in Slovenia are systemically regulated by the ZOUPAMO.

1.3. Definition of terms

Unless stipulated otherwise, the terms used in the guidelines have the same meaning as the terms used in the ZPPDFT-2. Within the framework of the guidelines, terms have the following meanings:

- an **obliged entity** is an entity that is an obliged entity in accordance with the first paragraph of Article 4 of the ZPPDFT-2, and for which Banka Slovenije is defined as a competent supervisory authority in accordance with the first paragraph of Article 164 of the ZPPDFT-2;
- a **competent supervisory authority** is a body responsible for conducting supervision of compliance with the requirements under the ZPPDFT-2, including compliance with the requirements relating to the assessment of ML/TF risks (Banka Slovenije, the FIU, the SMA);
- a **risk-based approach** is an approach in which the obliged entity identifies, assesses and understands the ML/TF risks to which it is exposed in its operations, and on this basis takes appropriate AML/CFT measures commensurate with the identified risks;
- **risk** is the probability of ML/TF events occurring;
- **risk criteria** are variables that either alone or in combination with others could increase or reduce ML/TF risks;
- **inherent risk** is the risk identified before the control environment is put in place;
- the **control environment** is the system of internal policies, procedures and controls put in place by the obliged entity with the aim of mitigating ML/TF risks;
- **residual risk** is the risk to which the obliged entity is exposed after the inherent risk and the effectiveness of the control environment have been assessed;
- the **obliged entity's risk assessment (OERA)** is an assessment in which the obliged entity analyses and assesses the inherent risk and the control environment, assesses the residual risk, and thus identifies the areas at the obliged entity that are more or less exposed to ML/TF risks, which forms the basis for adopting appropriate risk management measures;
- the **customer risk assessment (CRA)** is an assessment of risk criteria and an evaluation of whether an individual customer entails a lower or higher risk of abusing the obliged entity's system for ML/TF purposes;
- the **customer risk category** denotes the level of ML/TF risk posed by the customer with regard to the CRA;

- a **methodology** is a set of rules, procedures and algorithms that set out the manner in which individual risk criteria in the OERA or the CRA are taken into account;
- **private banking or wealth management** is a service offered by an obliged entity to wealthy and influential customers who execute transactions of very high value, to whom the obliged entity offers complex and individually tailored products and services, and who in light of all of this expect an appropriate measure of confidentiality and discretion in their transacting;
- **resident/non-resident** have the same meaning as in the law governing foreign exchange operations;
- a **domestic PEP** is a PEP who holds a function that is deemed a visible public position appointed by the Republic of Slovenia (e.g. the president, a minister, an ambassador or the Republic of Slovenia to another country, the CEO of a state-owned firm);
- a **foreign PEP** is a PEP who holds a function that is deemed a visible public position appointed by another EU Member State, a country of the EEA or a third country (e.g. the prime minister of a foreign country, a minister of a foreign country, a foreign ambassador to the Republic of Slovenia, the CEO of a state-owned firm of another EU Member State, EEA country or third country);
- the **list of high-risk countries** is a list published on the FIU's website within the framework of the List of countries in connection with which there is a high or increased risk of money laundering or terrorist financing, and encompasses the countries whose strategic deficiencies in the area of ML/TF pose a serious threat to the financial system of the EU, as a result of which the European Commission has placed them on the aforementioned list pursuant to Article 10 of the AMLD by virtue of a delegated act;
- the **list of increased-risk countries** is a list published on the FIU's website within the framework of the List of countries in connection with which there is a high or increased risk of money laundering or terrorist financing, and encompasses the countries in connection with which there is an increased risk or greater likelihood of ML/TF, as a result of which various international organisations have placed them on their lists of countries with increased risk;
- a **third country** is a country that is neither an EU Member State nor a signatory to the EEA Agreement (Norway, Iceland and Lichtenstein at the time of issuance of the guidelines);
- **non-face-to-face due diligence** means the entry into a business relationship or the execution of an occasional transaction where the customer is not physically present, i.e. at the same physical location as the obliged entity and the person acting on behalf of the obliged entity (employee, agent);
- a **dormant account** is an account in which the customer has not executed any transactions for a period of more than 12 months (interest and account management costs do not count as customer transactions);
- **P2P** (peer-to-peer) means the exchange of data or funds between two individuals without the intermediation of a third party;
- a **tumbler** (or mixer) is a type of anonymising service that obscures the chain of transactions in a blockchain by pooling together transactions at the same virtual currency address then spitting them back in a way that makes it appear as though they were sent from another address.

2. Risk assessment

2.1. General information about risk assessment

ML/TF risk is the risk that a customer will use the financial system for ML or TF, or the risk that a certain business relationship, transaction, product, service or distribution channel, having regard for the geographical risk factor, will be used directly or indirectly by the customer for ML/TF (first paragraph of Article 18 of the ZPPDFT-2).

Under the ZPPDFT-2, an obliged entity is required to assess ML/TF risks in its operations, and on this basis is required to put in place policies, procedures and controls for the effective mitigation of ML/TF risks, and in so doing is required to carry out customer due diligence measures as one of the key AML/CFT tasks.

By carrying out customer due diligence measures, obliged entities obtain information about the customer, and in conjunction with information about the services, products and distribution channels used by the customer as part of the business relationship are able to assess the degree to which the customer poses an ML/TF risk (the **customer risk assessment or CRA**).

The purpose of the CRA is adequate management of the risks posed to the obliged entity by a particular customer. Based on the CRA, the obliged entity determines the type of customer due diligence (standard, enhanced or simplified), which consequently has an impact on the frequency of the monitoring of the customer's transactions, including the procedure of the regular review and updating of the information and documentation obtained about the customer.

In addition to risk assessment at the level of the individual customer, obliged entities also draw up an **obliged entity's risk assessment (OERA)**, in which groups and types of customers, transactions, products, services and distribution channels are analysed and assessed (inherent risk), and in which the effectiveness of the existing control environment is assessed and the residual risk is calculated. On the basis of the OERA, obliged entities identify the ML/TF risks inherent in their operations, which forms the basis for adopting appropriate measures to reduce the identified ML/TF risks.

Obliged entities apply the principle of proportionality in their risk assessments (CRA and OERA), in accordance with which they tailor the AML/CFT measures to the nature and scale of their operations (and also the sectoral guidelines in greater detail).

2.1.1. Obliged entity's responsibility

Under the risk-based approach, the **CRA should reflect the customer's attributes and transactions**, while the **OERA should reflect the obliged entity's attributes and business**.

Obliged entities that have branches and subsidiaries under majority ownership are also required to formulate a group OERA, taking account of the OERAs of the individual undertakings making up the group that are required to take AML/CFT measures. **Obliged entities that are part of a group** take account of the parent undertaking's OERA.

Obliged entities define and document the **methodology for drawing up the OERA**, and also the **OERA** on each occasion.

In their internal policies obliged entities define the **methodology for drawing up the CRA**, and the risk criteria taken into account by obliged entities when formulating CRAs.

The OERA and the internal policies referred to in the previous paragraph must be **approved by the obliged entity's senior management**.

In addition the obliged entity must ensure that its employees have been made aware of the OERA and the risk criteria that affect the CRA, and how these affect their work. The obliged entity is required to provide regular professional training for all employees performing AML/CFT tasks (second paragraph of Article 87 of the ZPPDFT-2). The aim of employee training is to strengthen the awareness and proper understanding of ML/TF risks, and to ensure that employees perform their AML/CFT tasks effectively.

2.1.2. Updating of risk assessment

Risk assessment is not a one-off event, but a continuous process. Obliged entities must regularly update the risk assessment, particularly when taking account of changes in:

- the (external) environment in which the obliged entity operates;
- regulations;
- ML/TF techniques and trends;
- the obliged entity's internal environment.

Accordingly obliged entities are required to provide for the regular review and updating of the OERA and the CRA internal policies, including the risk criteria affecting the CRA. In so doing obliged entities must provide for the following at least (*see also Section 6 Sectoral guidelines for individual obliged entities*):

a) the updating of the **OERA once a year**, by **31 March**, with the information for the previous year;
b) the review and updating of the risk criteria and the **CRA** methodology **at least every two years**;
c) the updating of the OERA, the CRA methodology and the risk criteria before a significant change, such as the introduction of a new product (e.g. allowing e-money to be spent via a payment card), a change in business practice (e.g. abolishing points of sale and changing over to non-face-to-face transactions), new distribution channels (e.g. video-based electronic identification or other identification methods), or the use of new technologies (e.g. the use of innovative technologies in IT support for transaction monitoring), or in the event of organisational changes (e.g. the acquisition or merger of several obliged entities and the necessary reorganisation of the AML/CFT function). An update is not required if the obliged entity judges that the impact of the change on the OERA, the CRA methodology and the risk criteria is insignificant.

2.2. Obliged entity's risk assessment

The obliged entity's risk assessment (OERA) is **an aid to the obliged entity in understanding which business lines are exposed to higher risk of potential abuse from the perspective of ML/TF, and in which business lines it is necessary to strengthen the control environment to successfully manage ML/TF risks.** In its Guidelines on sound management of risks related to money laundering and financing of terrorism,[1] the BCBS also states that effective management of ML/TF risks requires the prompt identification and assessment of risks at the level of the obliged entity, and the preparation and implementation of appropriate policies, procedures and controls commensurate with the level of the identified risk.

Article 18 of the ZPPDFT-2 stipulates that the obliged entity is required to define and assess risks related to individual groups or types of customers with whom it has entered into business

[1] https://www.bis.org/bcbs/publ/d405.pdf

relationships; the geographical regions from which customers come or with which the obliged entity's transactions are related; the products and services that it offers; the transactions that it provides; and the distribution channels via which it provides its products and services. Having regard for their characteristics (in particular the size, type and scale of transactions, and the diversity of customer and business relationships), obliged entities are also required to define and assess the risks inherent in their own operations for the effective definition and assessment of the individual risks referred to in Article 18 of the ZPPDFT-2.

The OERA is used for the following purposes:

- an aid to the obliged entity's senior management in determining whether an effective system of ML/TF risk management has been put in place in all business lines and in all business processes;
- a basis for developing an appropriate strategy to mitigate the identified ML/TF risks (*e.g. overhauling AML/CFT policies and procedures, ensuring adequate human resources, allocating appropriate assets, ensuring a technological upgrade*).

In the OERA the obliged entity takes account of the risk criteria at the level of groups or types of customers, products, services, transactions, geographical regions and distribution channels (**inherent risk**), and the **control environment** put in place. The obliged entity also takes account of other risk criteria that could have an impact on the OERA, such as sovereign risk, sectoral risks and the obliged entity's future strategy (*e.g. expansion of the business network, new products, recruitment*).

The preparation of the OERA methodology and the execution of the OERA itself actively involves the AML/CFT officer, who has the requisite information and professional expertise to assess whether the OERA accords with the nature and scale of the obliged entity's operations. Here a key role is also played by the employees, who in accordance with the ZPPDFT-2 are required to provide support and assistance to the AML/CFT officer in providing the requisite information and documentation for the OERA. When the obliged entity assigns the preparation of the OERA in its entirety to another person or organisational unit at the obliged entity, or to an external contractor, the AML/CFT officer is required to review the OERA and the information that formed the basis for its preparation, and to assess whether the OERA presents a true picture of the situation at the obliged entity.

Irrespective of whether the obliged entity prepares the OERA itself or uses an external contractor, the **OERA must reflect the attributes of the obliged entity and its operations**.

In accordance with the principle of proportionality, obliged entities that do not offer complex products or services and whose exposure to ML/TF risks is low do not need a complex or extensive OERA. The definition of obliged entities of this type and the minimum standards for assessing inherent risk and the areas based on which obliged entities assess the control environment are given in the sectoral guidelines (*see Section 6 Sectoral guidelines for individual obliged entities*).

2.2.1. OERA methodology

The OERA must encompass the entirety of the obliged entity's operations where it is exposed to ML/TF risks. The OERA consists of an **assessment of inherent risk** and an **assessment of the control environment put in place**, and is reflected in an **assessment of residual risk**.

OBLIGED ENTITY'S RISK ASSESSMENT

Inherent risk	Control environment	Residual risk
Customers	ML/TF risk management	On the basis of the assessments of inherent risk and the control environment, residual risk is assessed as follows: • **low risk** • **medium risk** • **increased risk** • **high risk**
	Policies and procedures	
Geographical regions	Customer due diligence	
	Reporting	
Products and services	Record-keeping and data storage	
	AML/CFT function	
Transactions	Identification and reporting of suspected ML/TF	
	Monitoring and internal controls	
Distribution channels	Training	
	Independent auditing	
Other risks	Supervisory measures	

The OERA depends on the size of the obliged entity, the nature of its operations and its risk take-up policy, and consequently on the controls put in place with regard to risks (*see Section 6 Sectoral guidelines for individual obliged entities*).

The **criteria for assessing inherent risk and the areas based on which obliged entities assess the control environment** are cited below. The cited inherent risk criteria and criteria in the areas of the control environment are taken into account by obliged entities in the extent and with the content that is relevant to them. Obliged entities expand the suggested set of criteria with regard to their own ML/TF risks.

2.2.1.1. Inherent risk

Inherent risk is the risk to which the obliged entity is exposed before the control environment has been put in place. In assessing inherent risk, the obliged entity analyses risk criteria, which can be combined into the following groups:

- **Customer risk criteria**

The obliged entity analyses the number of customers with regard to the customer type or group, which it classifies according to the following risk criteria:

- CRA customers (*e.g. number of customers classified into the customer risk categories of low risk, medium risk or high risk*);
- customer status (*e.g. number of residents, non-residents; number of PEPs; number of undertakings listed on a securities market, public administration bodies and public enterprises*);
- customer activities (*e.g. number of undertakings engaged in high-risk industry or whose business activities are high-risk*);
- customer reputation (*e.g. number of enquiries or asset freeze requests received from the FIU in respect of the customer*);
- customer behaviour (*e.g. number of reports of suspected ML/TF in respect of the customer*).

- **Country risk criteria**

The obliged entity analyses the extent to which it does business with customers that have connections with higher- or lower-risk geographical regions, with regard to:

- the customer's registered office or domicile or temporary residence (*e.g. number of customers that have a registered office or a domicile or temporary residence in a geographical region that poses a low risk, medium risk, increased risk or high risk; number of customers that have a registered office or a domicile or temporary residence in a country subject to restrictive measures or in a country on the list of high-risk third countries*);

- the customer's nationality (*e.g. number of customers that are nationals of a geographical region that poses a low risk, medium risk, increased risk or high risk; number of customers that are nationals of a country subject to restrictive measures or of a country on the list of high-risk third countries*).

- **Product/service/transaction risk criteria**

The products, services and transactions that the obliged entity offers to customers may have a material impact on ML/TF risks. The volume of business in individual types of product and service is therefore taken into account within the framework of this group:

a) products:
   - accounts (*e.g. volume of business in current accounts of residents/non-residents, volume of business in e-banking accounts, volume of business in savings accounts and trading accounts*);
   - cards (*e.g. volume of business in prepaid cards*);
   - deposits (*e.g. stock of deposits*);
   - loans (*e.g. customers of mortgage loans, consumer loans, bridging loans*);
   - other products offered by the obliged entity;

b) services (*e.g. volume of business in remittance transfer services via Western Union / MoneyGram agents; trade finance; other services offered by the obliged entity*);

c) transactions: the volume of transactions is taken into account with regard to the risk of geographical regions and also with regard to other risk criteria (*e.g. volume of transactions related to a geographical region with low risk, medium risk, increased risk or high risk; volume of cash operations*).

- **Distribution channel criteria**

Certain distribution channels pose a higher ML/TF risk, and therefore should be taken into account as appropriate in the assessment of inherent risk. Here the number of customers that have entered into a business relationship with the obliged entity via an individual distribution channel is relevant (*e.g. business relationships entered into in person, via a third party, via electronic identification means, through video-based electronic identification, or through other approaches to the establishment and verification of identity*).

- **Other risk criteria**
   - size of the obliged entity (*e.g. headcount, number of offices, branches and subsidiaries*);
   - geographical exposure of the obliged entity (*e.g. registered office of the parent undertaking, registered office of branches and subsidiaries*);
   - HR changes at the obliged entity (*e.g. in front-office departments, back-office departments in the position of AML/CFT officer*);
   - the IT support put in place for AML/CFT (*e.g. who the support was developed by, how hits are processed, whether hits are processed promptly)*;
   - sectoral risk (*e.g. as proceeds from supranational and national risk assessment*).

Given the different nature and approach to business, the inherent risk at obliged entities referred to in points 1 and 2 of Section 1.2 Scope of application is determined for each business line, namely for:

- **Personal banking**, which encompasses the offer of various products and services to customers who are natural persons, other than natural persons who pursue business activities on the market (e.g. sole traders, persons pursing registered business activities);
- **Private banking**, as defined in Section 1.3 Definition of terms;

- **Small business banking**, which encompasses transactions with SMEs and natural persons who pursue business activities on the market (e.g. sole traders, persons pursing registered business activities);
- **Corporate banking**, which encompasses transactions with large enterprises and financial institutions that do not belong to any of the aforementioned business lines;
- **Correspondent banking**, which encompasses the provision of direct account or correspondent products and services to financial institutions and large enterprises;
- **Investment banking**, which encompasses the provision of investment services and transactions as defined in the ZTFI-1.

This demarcation allows the obliged entity to identify risks not only at the level of the obliged entity, but also at the level of the individual business line. Accordingly the obliged entity can act faster to eliminate any ML/TF risks identified through measures that suit the individual business line's way of doing business. In accordance with the principle of proportionality, demarcation into business lines is not required for all obliged entities (*for more detail, see Section 6 Sectoral guidelines for individual obliged entities*).

In the OERA the obliged entity takes account of the risk criteria cited above, at a minimum, and also those that it judges could have an impact on its exposure to ML/TF risks. The obliged entity defines additional risk criteria within the individual groups, or includes additional business lines in the analysis, if this is necessary in light of the attributes of its operations.

After analysing the risk criteria, the obliged entity **assesses the inherent risk**, whereby the inherent risk is assessed as low when the criteria do not pose any major risks, or as high when the majority of the risk criteria pose a high risk.

Inherent risk level	Assessment
Low risk	1
Medium risk	2
Increased risk	3
High risk	4

The obliged entity draws up its own methodology for assessing inherent risk such that the OERA reflects the specific attributes of its operations.

2.2.1.2. Control environment

Once the inherent risk has been assessed, it is necessary to determine the extent to which the control environment put in place is effective. With regard to the control environment, account is taken of policies and procedures, and also of the controls conducted by employees at the first level (organisational units), at the second level (the AML/CFT officer), and the third level (the internal audit department).

When assessing the control environment, the obliged entity analyses the risk criteria deriving from its policies, procedures and controls within the framework of the following areas (*see Section 6 Sectoral guidelines for individual obliged entities*):

- **ML/TF risk management**

The senior management is responsible for putting in place an effective system of risk management in the area of AML/CFT. Accordingly it must establish and promote a culture of risk management (tone from the top) that ensures adequate awareness on the part of all employees, and consistent observation of the defined policies and procedures (*e.g. how formal and informal lines of reporting on ML/TF risks are put in place, the proper positioning of the AML/CFT function in the obliged entity's organisational structure, whether the AML/CFT function is recognised as a key function*).

- **Policies and procedures**

The compliance of the obliged entity's internal policies with the requirements of law and the guidelines of the competent supervisory authorities is examined. Within the framework of the OERA the obliged entity also examines whether its internal policies and procedures ensure the adequate management of the identified inherent risks (*e.g. whether the internal AML/CFT policies have been updated in line with the requirements of law and the guidelines of the competent supervisory authorities, whether the obliged entity has implemented the policies of the group in timely fashion*).

- **Customer due diligence**

Customer due diligence is one of the basic AML/CFT measures. An assessment is made of the adequacy of the controls through which the obliged entity ensures that customer due diligence measures are being consistently implemented, and any deficiencies identified are being rectified (*e.g. irregularities in customer due diligence, irregularities in the implementation of controls, irregularities identified in the CRA*).

- **Reporting**

In addition to the appropriate status and positioning of the AML/CFT function within the obliged entity's organisational structure (as defined in the area entitled AML/CFT function), the establishment of adequate reporting flows is also extremely important for the effective performance of the AML/CFT officer's tasks. Within the framework of the assessment of the control environment, checks are made to establish whether reporting lines have been put in place between the AML/CFT officer and the senior management (*e.g. frequency of reporting to the senior management by the AML/CFT officer*), and between the AML/CFT officer and employees responsible for the direct performance of tasks (*e.g. frequency of reporting by business units to the AML/CFT officer*) or supervision of the performance of tasks in the area of AML/CFT (*e.g. frequency of reports by area coordinators*).

- **Record-keeping and data storage**

The obliged entity assesses whether records of information about customers, business relationships and transactions executed within the framework of a business relationship, and occasional transactions, and records of data reported to the FIU are being properly provided. The obliged entity also assesses whether employees are properly storing information and documentation obtained about customers for ten years after the execution of a transaction or after the termination of the business relationship, and other data required by law (*e.g. deficiencies in the storage of data obtained during customer due diligence; adequacy of records of data reported to the FIU*).

- **AML/CFT function**

The positioning of the AML/CFT function in the organisational structure, the number of employees performing AML/CFT tasks as their sole work duty (AML/CFT officer, deputy-officers), and the number of people performing such tasks in addition to their regular tasks (deputies, area coordinators) are reviewed. On this basis an assessment is made of the

adequacy of human resources and organisation in the area of AML/CFT with regard to the inherent risk to which the obliged entity is exposed (*e.g. whether the obliged entity has appointed an AML/CFT officer, whether the AML/CFT officer / deputy-officer exclusively performs tasks in the area of AML/CFT, whether area coordinators perform their work effectively and with the requisite quality*).

- **Identification and reporting of suspected ML/TF**

The AML/CFT system put in place must ensure that the obliged entity is able to identify suspicious transactions promptly and report them to the FIU. An assessment is also made of the effectiveness of the system for identifying deviations from usual transactions and the effectiveness of the procedures for further treatment of unusual transactions, which form the basis for identifying suspicious transactions and reporting suspected ML/TF to the FIU (*e.g. adequate functioning of software support for identifying unusual transactions, adequate treatment of flagged deviations, timely reporting to the AML/CFT officer or the FIU*).

- **Monitoring and internal controls**

The obliged entity is required to provide for regular internal controls over the performance of AML/CFT tasks. Here an assessment is made primarily of the effectiveness of the controls put in place at the second level, for which the AML/CFT officer is responsible (*e.g. number of second-level controls conducted, quality of second-level controls, realisation of planned controls*).

- **Training**

The obliged entity is required to provide regular professional training for all employees performing tasks that relate in any way to AML/CFT. The assessment of the control environment in this segment includes an assessment of whether the annual training plan has been realised, whether all target groups of participants have been included in training, and whether the topics covered by training correspond sufficiently to the inherent risks to which the obliged entity is exposed (*e.g. realisation of annual training plan, number of participants in training*).

- **Independent auditing**[2]

The internal audit department conducts independent reviews of AML/CFT system for the purpose of identifying any deficiencies and strengthening the obliged entity's existing policies, procedures and controls. An assessment is made of whether the reviews conducted by the internal audit department have identified material deficiencies or breaches that show that it is necessary to strengthen the control environment (*e.g. frequency of AML/CFT audits, identified breaches, rectification of breaches*).

- **Supervisory measures**

The analysis of the control environment also needs to include potential inspections by competent supervisory authorities in the area of AML/CFT, and their supervisory measures (*e.g. whether an inspection has been conducted by a competent supervisory authority, identified breaches, rectification of breaches*).

[2] Obliged entities that are medium-size or large enterprises in accordance with the ZGD-1 are required to put in place an independent internal audit department to verify internal policies, controls and procedures (point 2 of second paragraph of Article 20 of the ZPPDFT-2). Here it should additionally be clarified that merely putting in place a unit at the obliged entity does not necessarily meet the requirement for the independence of the audit function; rather the objective of the provision is that audit should be functionally independent, i.e. not subject to the (undue) influence of another or of the obliged entity that it is auditing.

In analysing the control environment the obliged entity takes account of the areas cited above, and the risk criteria that it judges have an impact on its ML/TF risks, whereby the areas may be broken down into more detailed individual risk criteria, and additional areas may be included in the analysis.

After analysis of the risk criteria has been conducted in individual areas of the control environment, **it is then necessary to assess the control environment**. Controls that are conducted effectively, regularly, and without any identified deficiencies are assessed as "good", while controls that are either ineffective or non-existent are assessed as "poor".

Assessment of the control environment	Assessment
Good control environment	1
Acceptable control environment	2
Deficient control environment	3
Poor control environment	4

The obliged entity is required to draw up its own methodology for assessing the control environment such that the OERA reflects the specific attributes of its operations.

While the analysis and assessment of inherent risk involves quantitative data in connection with the risk criteria (number and volume), the assessment of the control environment is qualitative in nature. **For this reason, after completing the analysis and assessment of inherent risk and the control environment, the AML/CFT officer has the option of proposing that individual areas of the control environment be assessed more or less strictly** than defined in the OERA methodology (*e.g. controls are conducted less frequently, but prove to be effective*). The AML/CFT officer may propose a change to the assessment of the control environment on the basis of expert judgment, having regard for the attributes of the entire AML/CFT system at the obliged entity. Any change in the assessment of the control environment proposed by the AML/CFT officer must be clearly documented, and must be approved by the obliged entity's senior management.

2.2.1.3. Residual risk

The obliged entity assesses residual risk on the basis of the analysis and assessments of inherent risk and the control environment (**residual risk assessment**). The residual risk assessment makes the obliged entity aware of whether the system put in place provides for effective detection and prevention of ML/TF, or whether improvements are required.

The residual risk assessment is expressed as one of four levels:

- **Low residual risk**

  Residual risk is assessed as low when the **inherent risk** at the level of the obliged entity is assessed as **low** or **medium**, while the **control environment** is assessed as **good** or **acceptable**.

- **Medium residual risk**

  Residual risk is assessed as medium when:
  - the **inherent risk** is assessed as **low**, while the **control environment** is assessed as **deficient** or **poor**;
  - the **inherent risk** is assessed as **high** or **increased**, while the **control environment** is assessed as **good**;
  - the **inherent risk** is assessed as **medium**, while the **control environment** is assessed as **acceptable**.

- **Increased residual risk**

Residual risk is assessed as increased when the **inherent risk** is assessed as **medium** or **increased**, while the existing **control environment** is assessed as **deficient** or **poor**. Residual risk is also assessed as increased when the **inherent risk** is assessed as **high** or **increased**, but the **control environment** put in place is assessed as **acceptable**.

- **High residual risk**

Residual risk is assessed as high when the **inherent risk** at the level of the business line or the obliged entity is assessed as **high** or **increased**, while the **control environment** put in place is assessed as **deficient** or **poor**.

OBLIGED ENTITY'S RISK ASSESSMENT					
RESIDUAL RISK ASSESSMENT		**Control environment**			
		Good	**Acceptable**	**Deficient**	**Poor**
Inherent risk	**High**	MR	IR	HR	HR
	Increased	MR	IR	IR	HR
	Medium	LR	MR	IR	IR
	Low	LR	LR	MR	MR

The AML/CFT officer may propose that the residual risk assessment be raised or lowered by a maximum of one level (*e.g. a projected merger with another obliged entity*). The grounds for changing the residual risk level must be documented and must be approved by the obliged entity's senior management.

The obliged entity puts in place its own methodology for assessing residual risk, and must take account of the following in so doing:

- the residual risk assessment should have no more than five and no fewer than three risk levels;
- residual risk may not be assessed as low when the inherent risk is assessed as high;
- residual risk may not be assessed as low when the control environment is assessed as poor.

2.2.2. Obliged entity's measures on the basis of the OERA

After the OERA is conducted, the next activities are as follows:

1. **The obliged entity documents the OERA**: it defines the risk criteria based on which it analyses and assesses the inherent risk and the control environment, describes the methodology for assessing inherent risk, the control environment and residual risk, and any grounds for deviations from the assessment of the control environment or residual risk.
2. Once the OERA has been documented, it is **approved by the obliged entity's senior management**.
3. The responsible employees at the obliged entity (the AML/CFT officer, the responsible management board members, or other employees) **present the results of the OERA to the persons responsible** for individual business lines and to the **internal audit department**. In accordance with the principle of proportionality, the aforementioned requirement is regulated differently for individual obliged entities (*for more detail, see Section 6 Sectoral guidelines for individual obliged entities*).

4. On the basis of the OERA, the obliged entity draws up **ML/TF risk management measures** as illustrated below.

On the basis of the level of residual risk identified within the framework of the OERA, the obliged entity draws up measures to mitigate any ML/TF risks identified at the obliged entity. If deficiencies in the control environment (*e.g. deficient policies or procedures*) or high inherent risk that the obliged entity is unable to adequately manage (*e.g. delays in the treatment of flagged deviations from usual transactions*) were identified during the OERA, it is necessary to draw up an **action plan for the rectification of the identified irregularities, and to set a deadline by which the deficiencies must be rectified**. Identified deficiencies must be rectified by a reasonable deadline, or by no later than the time of the next OERA.

The residual risk level in the OERA also affects the **obliged entity's strategy** in the area of AML/CFT, and in the business line. When making decisions as to whether to introduce additional products or services, whether to establish new distribution channels, or whether it is necessary to upgrade the existing control environment in this connection (*e.g. additional staff, IT investment*), the obliged entity takes account of the findings of the OERA.

The OERA also affects the **obliged entity's customer acceptance policy**, i.e. whether it will accept higher-risk or lower-risk customers in light of the identified inherent risk and the control environment put in place. This is a business decision on the part of the obliged entity, which has a significant impact on the implementation of AML/CFT measures at the level of the obliged entity (*e.g. additional employee training, a reduction in existing controls for lower-risk customers*) and also at the level of the individual customer.

2.3. Customer risk assessment

Based on the customer risk assessment (CRA), the obliged entity determines the type of due diligence (enhanced, simplified, standard) and the method of monitoring the customer's business activities. Here the principle of proportionality applies, in line with which (having regard for the CRA) higher-risk customers are subject to more frequent and broader-scope controls, while lower-risk customers are subject to less frequent and narrower-scope controls.

Undertaking the CRA in the area of ML/TF risks necessitates the following:

- identifying the risk criteria, and
- determining the materiality of each individual risk criterion or its impact on the CRA.

Risk criteria are presented below **with regard to the level of ML/TF risks** (LR, MR, IR, HR) that entail a minimum standard, whereby individual obliged entities uphold minimum standards as defined in the sectoral guidelines (*for more detail, see Section 6 Sectoral guidelines for individual obliged entities*).

The obliged entity may take account of additional risk criteria, or may treat them more strictly. In the definition of additional risk criteria, obliged entities referred to in points 1 to 5 of Section 1.2 Scope of application uphold the ML/TF risk factors guidelines.

Because the **risk-based approach** is used in the CRA, an individual risk criterion does not yet necessarily mean the allocation of the customer to a customer risk category of low risk or high risk, unless this is explicitly stipulated in the ZPPDFT-2 and the guidelines (a risk criterion of "HR" automatically assigns the customer to the customer risk category of "high risk").

2.3.1. Risk criteria

The obliged entity defines risk criteria with regard to individual types of risk inherent in:

- the customer itself;
- the geographical region;
- the products, services or transactions;
- the distribution channels via which the obliged entity offers products or services;
- other risks.

2.3.1.1. Customer risk

Customer risk is the risk inherent in:

- the **customer's activities**, which is closely related to the monitoring of the purpose and scale of the transactions at the obliged entity. For natural persons, the vital information is therefore employment status (*e.g. the size of the payments is dependent on the employer and the job, pensioner, student, unemployed*), while for legal persons it is information about the business activities (the principal business activity for which the legal person is registered in the business register) or the industry in which it is engaged;
- the **customer's status**, which for natural persons is related to the function that they perform within the framework of employment or activities on behalf of an interest group (*e.g. president of a political party [PEP]*), while for legal persons it is related to their status (*e.g. concerns, foundations, associations and other forms of partnership that expose the customer to higher risk*);
- the **customer's reputation**, which is related to "**negative information**" that the obliged entity holds about the customer:
    - on the basis of publicly available data (*the media, information from the environment, where the assessment of this information should also take account of the reliability and credibility of the source, e.g. negative information includes i) media stories about the final conviction of person XY for the criminal offence of ML or an economic crime, but not online chatter on the alleged offences of person XY; ii) when it is publicly known that the customer or BO is the subject of investigation or has been convicted of terrorist acts or that the customer lives with or is otherwise closely linked to such a person);*
    - on the basis of internal information (*e.g. the customer embezzled a bank instrument, an enquiry against the customer has been received from the FIU*);
- the **customer's behaviour**, particularly unusual or suspicious behaviour by the customer before entering into the business relationship (*e.g. the customer does not wish to disclose information required by law*) or during the business relationship (*e.g. the customer does not wish to provide additional evidence*).

The obliged entity also takes account of **risks in connection with parties related to the customer** (statutory representatives, authorised representatives, BO).

The set of **customer risk criteria** that the obliged entity must take into account as the minimum standard is cited below, although the obliged entity may also take account of additional criteria or treat the below criteria more strictly (see *Section 6 Sectoral guidelines for individual obliged entities*).

CUSTOMER LEGAL/NATURAL PERSON	CUSTOMER RISK CRITERIA	RISK LEVEL
NP/LP	The customer is a resident	LR
LP	An undertaking listed on a securities market to which disclosure requirements and requirements for adequate transparency of the BO apply	LR

LP	A credit or financial institution established in an EU Member State or a third country that has put in place adequate AML/CFT mechanisms	LR
LP	Public administration bodies and public enterprises in the Republic of Slovenia	LR
LP	An undertaking under 100% ownership of the Republic of Slovenia	LR
NP/LP	The customer is a non-resident	MR
LP	Undertakings that disclose ownership on the basis of bearer shares, where the ownership is evident from the record of holders of bearer shares at KDD	MR
LP	Other undertakings that are not classed as high-risk or low-risk	MR
NP	The customer's identity was verified on the basis of a temporary residence permit or an asylum-seeker's ID card	IR
NP/LP	The customer's statutory representative, authorised representative or BO is a PEP, a close family member of a PEP, or a close associate of a PEP	IR
NP/LP	Negative information has been obtained in connection with the customer, its statutory representative, its authorised representative or the BO	IR
NP/LP	Indicators of suspected ML/TF have been flagged in connection with the customer or a related party, for example: ▪ the customer or a related party is behaving unusually or suspiciously; ▪ the customer has failed to provide adequate clarifications with regard to the economic logic of the envisaged transactions; ▪ there is doubt as to the credibility or relevance of the submitted documentation; ▪ the customer requests secrecy when entering into the business relationship, and does not wish to disclose the requisite information during due diligence	IR
NP/LP	An enquiry has been received from the FIU for the customer, its statutory representative, its authorised representative or the BO	IR
LP	Undertakings operating in the following industries or whose business activities are as follows:[3] • money services business; • virtual currency services or other transactions included in such services; • non-governmental and non-profit organisations; • charitable organisations; • manufacturers and traders of armaments and other military equipment; • mining and quarrying; • petroleum and natural gas; • construction; • pharmaceuticals; • sale and brokerage of real estate; • sale of gold and other precious metals; • sale and brokerage of valuable goods and high-value assets (e.g. yachts, cars, works of art and antiques); • casinos and other games of chance (betting shops, online games of chance, etc.).	IR
LP	Sudden changes in the ownership structure or ultimate BO that cannot be explained	IR
LP	The undertaking's ownership structure is unusual or overly complicated relative to the nature of its business	IR
LP	The customer is a legal person or another entity of foreign law established for a specific purpose (a special-purpose vehicle [SPV] or trust)	IR
LP	There is credible information about a credit institution, financial institution or other legal person that is required to implement AML/CFT measures that supervisory measures for the rectification of irregularities in the area of	IR

[3] When identifying a legal person's higher-risk business activities, obliged entities may make use of various resources (e.g. the standard classification of activities [SKD] or the European classification of economic activities [NACE] that are classed as higher-risk activities and industries; CNVOS's list of NGOs; the register of humanitarian organisations; the register of providers engaged in exchange services between virtual currencies and fiat currencies and custodian wallet providers administered by the FIU). In the CRA the obliged entity also takes account of information about an undertaking's industry or business activities that pose an increased risk, if the information is obtained from the customer or is identified (or should be identified with regard to the available information) as part of transaction monitoring.

	AML/CFT or administrative fines have been imposed on it by supervisory authorities	
NP/LP	The customer or the BO is a PEP, a close family member of a PEP, or a close associate of a PEP	HR
NP/LP	The customer, its statutory representative, its authorised representative or the BO has been reported to the FIU for suspected ML/TF	HR
NP/LP	The FIU has submitted a transaction monitoring request or an asset freeze request for the customer	HR
NP/LP	The customer, its statutory representative, its authorised representative or the BO is on a list of persons, groups and entities involved in terrorist acts to whom EU restrictive measures apply (e.g. FBE)	HR
LP	Undertakings that disclose ownership on the basis of bearer shares, where the customer discloses ownership on the basis of a contract, notarial protocol or share register of a foreign authority	HR

2.3.1.2. Country risk

Increased risk is posed by countries and geographical regions that have weak AML/CFT systems, countries with a high degree of corruption or criminal activity, and countries against which international organisations have imposed restrictive measures. The obliged entity also takes account of the country risk of customers and related parties in the CRA (*if the information is available given the scope of the due diligence*), in particular:

- for natural persons, the nationality and region of domicile and temporary residence;
- for legal persons, the registered office and the geographical region where the main place of business is located, if different from the registered office;
- for the statutory representative, the authorised representative and the BO, the nationality and the region of domicile and temporary residence (*if the information is available given the scope of the due diligence*).

The set of **country risk criteria** that the obliged entity must take into account as the minimum standard is cited below, although the obliged entity may also take account of additional criteria or treat the below criteria more strictly (see *Section 6 Sectoral guidelines for individual obliged entities*).

CUSTOMER LEGAL/NATURAL PERSON	COUNTRY RISK CRITERIA	RISK LEVEL
NP/LP	The customer, statutory representative, authorised representative or BO is a national of a country that is assessed as a **low risk** (EU Member States or third countries with an effective AML/CFT system and a low level of corruption and other criminal activity)	LR
NP/LP	The customer, statutory representative, authorised representative or BO has a registered office or domicile or temporary residence in a country that is assessed as a **low risk** (EU Member States or third countries with an effective AML/CFT system and a low level of corruption and other criminal activity)	LR
NP/LP	The customer, statutory representative, authorised representative or BO is a national of a country that is assessed as a **medium risk** (the country is not assessed as a low, increased or high risk)	MR
NP/LP	The customer, statutory representative, authorised representative or BO has a registered office or domicile or temporary residence in a country that is assessed as a **medium risk** (the country is not assessed as low, increased or high risk)	MR
NP/LP	The customer, statutory representative, authorised representative or BO is a national of a country that is assessed as an **increased risk** (countries where there is higher probability of ML/TF; countries against which restrictive measures have been imposed by the UN Security Council or the EU)	IR
NP/LP	The customer, statutory representative, authorised representative or BO has a registered office or domicile or temporary residence in a country that is assessed as an **increased risk** (countries where there is higher probability of ML/TF;	IR

	countries against which restrictive measures have been imposed by the UN Security Council or the EU)	
NP/LP	The customer, statutory representative, authorised representative or BO is a national of a country that is on the list of high-risk third countries	IR
NP/LP	The customer, statutory representative, authorised representative or BO has a registered office or domicile at an address that is known to be fictitious (including PO boxes in the rest of the world)	IR
NP/LP	The customer, statutory representative, authorised representative or BO has a registered office, domicile or temporary residence in a country that is on the list of high-risk third countries	HR

Having regard for the ML/TF risks of the individual geographical region, the obliged entity **draws up and regularly updates its own list of geographical regions**; all countries in the world should be included on the list.

When assessing country risk obliged entities are recommended to use a variety of sources and a risk-based approach. In keeping with such an approach, an individual source should not determine the final assessment of country risk, unless so stipulated by the ZPPDFT-2. Obliged entities assess an individual geographical region as a **low risk, medium risk, increased risk or high risk**.

In accordance with the principle of proportionality, sectoral guidelines for individual obliged entities regulate the requirement for the obliged entity to draw up its own list and assessment of geographical regions differently (*for more detail, see Section 6 Sectoral guidelines for individual obliged entities*).

The **mandatory sources** that the obliged entity is required to take into account in the assessment of country risk are:

- the list of high-risk third countries (*see Section 1.3 Definition of terms*);
- the list of increased-risk countries (*see Section 1.3 Definition of terms*);
- list of countries against which restrictive measures have been imposed by the UN Security Council or the EU.[4]

The **additional sources** of information that it is reasonable to take into account in the assessment of country risk are:

- information from industry with regard to typologies and emerging risks with regard to geographical regions;
- information from international organisations and associations that assess countries across various criteria, such as mutual evaluation reports (*e.g. FATF, Moneyval*), reports on deficient taxation (*e.g. OECD*), reports on corruption (*e.g. Transparency International*) and other criminal activity (*e.g. UN FIU on Drugs and Crime*), IMF FSAP reports;
- the FATF blacklist and grey list;
- the status of a country's memberships of internationally recognised organisations active in the area of AML/CFT (FATF, Moneyval);
- information from credible and reliable open sources (*e.g. stories by reputable newspapers*);
- information obtained on the basis of credible and reliable commercial organisations (*e.g. Dow Jones, World Check, SWIFT*);
- supranational risk assessments by the European Commission;
- national risk assessments of individual countries;
- professional judgement and expertise (*e.g. knowledge of fictitious addresses*).

[4] Lists of countries against which restrictive measures have been imposed can be found on EU Sanctions Maps (https://sanctionsmap.eu/#/main).

2.3.1.3. Product/service/transaction risk

In respect of products, services and transactions, the obliged entity assesses risks related to:

- **transparency**: namely the extent to which products, services and transactions allow the customer or BO to remain anonymous or to conceal their identity;
- **complexity**: the extent to which a transaction is complex and whether it involves multiple parties or multiple jurisdictions (*e.g. trade finance*), or the extent to which products or services allow payments by third parties or accept overpayments that are not usually expected;
- **value or size**: the extent to which products, services or transactions are cash-intensive, and the extent to which they simplify or encourage high-value transactions.

In addition to new products and services, the obliged entity also takes account of the attributes of innovative solutions in providing a specific product or service (i.e. advanced market channels).

The set of **product/service/transaction risk criteria** that the obliged entity must take into account as the minimum standard is cited below, although the obliged entity may also treat the below criteria more strictly (*see Section 6 Sectoral guidelines for individual obliged entities*). In addition to the aforementioned products and services, the obliged entity **must** take account of and assess the risk of the remaining products and services that it offers in its own CRA methodology and in the individual CRAs.

CUSTOMER LEGAL/NATURAL PERSON	PRODUCT/SERVICE/TRANSACTION RISK CRITERIA	RISK LEVEL
NP/LP	Products that pose low ML/TF risk: • mortgage loans; • other purpose-specific retail loans, where the funds are paid out directly to the vendor of goods or the service provider; • deposits; • savings accounts; • current accounts aimed at a particular class of customers (pensioners' accounts intended for inward pension payments, children's savings accounts); • other products that the obliged entity has assessed as posing low ML/TF risk.	LR
NP/LP	Products and services that the obliged entity has assessed as posing medium risk	MR
NP/LP	Products that pose increased risk: • prepaid payment cards; • debit and credit cards with no limits on transactions; • cheques; • safe deposit boxes; • leasing and other credit agreements where the payer is a third party; • fiduciary accounts and accounts that allow account managers, attorneys and other entities to execute transactions on behalf of their clients via accounts at the bank; • other products that the obliged entity has assessed as posing increased ML/TF risk.	IR
NP/LP	Services that pose increased risk: • private banking; • investment banking; • trade finance; • services related to trading in precious metals (e.g. purchase of gold); • remittance services via agents (e.g. Western Union, MoneyGram); • other services that the obliged entity has assessed as posing increased ML/TF risk.	IR

NP/LP	Transactions that pose increased risk and are taken into account within the framework of transaction monitoring, and could have an impact on the CRA: • the customer mostly transacts in cash (including deposits and withdrawals at ATMs, which is unusual for its registered business activities); • transactions where the source of funds is not known; • transactions that do not have a clear economically or legally justified purpose; • the number of transactions deviates from the customer's usual volume of business; • the value of the transactions deviates from the customer's usual volume of business; • the transactions deviate from the stated purpose of business; • transactions in a previously dormant account; • smurfing; • inward and immediate outward transactions in similar or the same amounts; • other unusual circumstances in the execution of transactions (e.g. significant and unexplained geographical distance between the registered office of the obliged entity and the registered office of the customer, frequent and unexplained transfers of funds to different geographical regions); • transactions with countries on the list of increased-risk countries; • transactions related to countries on the list of high-risk third countries.	IR

2.3.1.4. Distribution channel

In this case there is an assessment of the risk of misuse for ML/TF purposes posed by the distribution channel via which the obliged entity offers products or services to the customer. The obliged entity must assess the following in particular:

- the extent to which the product or service is offered/provided without the customer being present in person; and
- whether the products or services are offered via third parties, and what the nature of the relationship between the obliged entity and the third party is.

The set of **distribution channel risk criteria** that the obliged entity must take into account as the minimum standard is cited below, although the obliged entity may also take account of additional criteria or treat the below criteria more strictly (see *Section 6 Sectoral guidelines for individual obliged entities*).

CUSTOMER LEGAL/NATURAL PERSON	**DISTRIBUTION CHANNEL RISK CRITERIA**	**RISK LEVEL**
NP/LP	The business relationship is entered into in the personal presence of the customer or the statutory representative	LR
NP/LP	The business relationship is entered into by means of electronic identification with a high degree of reliability	LR
NP/LP	The business relationship is entered into by means of video-based electronic identification	MR
NP/LP	The business relationship is entered into by other means of establishing and verifying identity	MR
NP/LP	The business relationship is entered into via an authorised representative	MR
NP/LP	The business relationship is entered into via an external service provider	MR
NP/LP	The business relationship is entered into via a third party	MR

2.3.2. CRA methodology

Obliged entities are required to formulate their own CRA methodology in which they:

- appropriately **evaluate the aforementioned risk criteria** (at the obliged entity), whereby they must have at least the risk level defined in the guidelines;
- **consider, define and evaluate any additional risk criteria (of their own)**, thus capturing all the attributes of their business in full;
- **set out a system for weighting the risk criteria**, having regard for the risk level of individual criteria, and, in line with the risk-based approach, ensure that the higher-risk criteria have a greater impact on the CRA;
- ensure that **risk criteria at high risk level automatically place the customer in the category of high-risk customers** (*e.g. PEPs, customer's links to a country on the list of high-risk third countries*);
- define the following customer risk categories at a minimum: **low risk**, **medium risk** and **high risk** (the obliged entity may define more customer risk categories, but the total number should not exceed five).

The obliged entity should ensure that its income in connection with an individual customer or with a particular product or service does not influence its CRA methodology. Neither should the methodology lead to a situation where it is impossible to place any customer in the high customer risk category.

Based on the CRA, the obliged entity places the customer into one of the customer risk categories, and adjusts its implementation of AML/CFT measures as appropriate (most notably the scope of due diligence and the monitoring of the customer's business activities), as is evident from the table below and as explained in detail below in the guidelines.

Customer risk category	Type of customer due diligence	Frequency of transaction monitoring[5]	Review and updating of information and documentation
Low risk	Simplified due diligence	Annual	3 to 5 years
Medium risk	Standard due diligence	Half-yearly	2 to 3 years
High risk	Enhanced due diligence	Monthly	1 to 2 years

Having regard for the principle of proportionality and approach to business, obliged entities referred to in point 5 of Section 1.2 Scope of application take account of the sectoral guidelines when drawing up the methodology (*for more detail, see Section 6.3 Sectoral guidelines for currency exchange operators*).

2.3.3. Definition of initial CRA and updating of CRA

The obliged entity is required to conduct customer due diligence before entering into a business relationship, within the framework of which it obtains, at a minimum, information of the scope set out by the ZPPDFT-2 (*e.g. the customer's registered office or domicile or temporary residence, nationality, information about PEPs*). Based on the information obtained about the customer, the

[5] Irrespective of the customer risk category, the obliged entity should ensure that individual high-risk transactions, based on the requirements of the ZPPDFT-2 or the obliged entity's own assessment, are monitored as they happen (*for more detailed information, see Section 4.1 Transaction monitoring*).

obliged entity conducts its **initial CRA**, and places the customer in the relevant customer risk category.

Based on the initial CRA, the obliged entity sets out the **scope of information and documentation** that it will request from the customer before entering into the business relationship or executing an occasional transaction. If a business relationship is entered into, it then determines the **type of transaction monitoring** and the **frequency of reviewing and updating the information and documentation about the customer**.

As part of the customer due diligence, the obliged entity must also provide for the regular and diligent monitoring of the customer's business activities, within the framework of which it assesses the **risk criteria deriving from the customer's transactions**, and also **changes to the basic information about the customer (updating of the CRA)**. During the business relationship it may prove to be the case that the customer poses a higher ML/TF risk than was evident from the information obtained when the business relationship was entered into. In general these are cases when the obliged entity placed the customer in the customer risk categories of low risk or medium risk when the business relationship was entered into, but the nature of the customer's actual transactions suggests increased ML/TF risk. In this case the obliged entity takes account of additional risk criteria when updating the CRA in accordance with its own CRA methodology, and **updates the customer risk category** as appropriate.

For the effective prevention of ML/TF risks, information about the customer risk category must be available at any time to employees at the obliged entity whose work duties involve ML/TF risk management. Accordingly obliged entities **are required to manage the information on customer risk category within the framework of their IT support**, which allows for the proper traceability of changes to the initial CRA. In accordance with the principle of proportionality, the aforementioned requirement is regulated differently for individual obliged entities (*for more detail, see Section 6 Sectoral guidelines for individual obliged entities*).

In accordance with the risk-based approach, various risk criteria with differing risk levels are taken into account during the CRA and consequently have various impact on the CRA. Obliged entities are therefore recommended to **put in place IT support that provides for the automatic execution of the CRA and definition of the customer risk category**. The system must also allow manual changes to the automatically defined customer risk category. The grounds for any manual change and the identity of the employee who entered the change in customer risk category must be recorded. In accordance with the principle of proportionality, the aforementioned requirement is regulated differently for individual obliged entities (*for more detail, see Section 6 Sectoral guidelines for individual obliged entities*).

3. Customer due diligence

The obliged entity obtains the minimum scope of information for defining the initial CRA during customer due diligence, and in so doing establishes and verifies the customer's identity and monitors the customer's business activities in accordance with the risk assessment determined.

3.1. Establishment and verification of customer's identity

The fundamental customer due diligence measure, even before the business relationship is entered into or the occasional transaction is executed, is **establishing and verifying the identity** of the customer, the statutory representative and the authorised representative. The obliged entity may establish and verify the identity of the customer and the related parties **in person**, or **on a non-face-to-face basis**.

Irrespective of whether the information is obtained in person or on a non-face-to-face basis, the identity of the customer and the related parties must be established and verified on the basis of **credible, independent and objective sources** (a valid personal identification document[6] or, if they do not have one, a temporary residence permit and an asylum-seeker's ID card[7]).

3.1.1. Customer due diligence in person

The obliged entity establishes and verifies the identity of a customer (natural person), a statutory representative, an authorised representative, a sole trader or an individual pursuing registered business activities by **examining their official personal identification document in their personal presence** (*see Section 1.3 Definition of terms*).

If the customer is being represented by a statutory representative or authorised representative, the obliged entity establishes and verifies the identity of the statutory representative or authorised representative in their personal presence, and simultaneously verifies the existence and basis of the statutory representation or the validity of the authorisation. The personal presence of a customer who is being represented by a statutory representative or authorised representative is not required. In this case the obliged entity obtains the information about the customer directly from the certified written authority or the basis for statutory representation (e.g. birth certificate, government authority decision). In this case the customer's identity is deemed to have been established in the certification process (e.g. by the notary, administrative unit, court, social work centre). The obliged entity then merely verifies the identity on the basis of the copy of the customer's personal identification document. Certification of the authorisation is not required when the customer signs the authorisation in the personal presence of the obliged entity's representative or by a qualified digital signature that can be deemed to be credible and adequate (Articles 30 and 31 of the ZPPDFT-2) by the obliged entity from the perspective of data completeness, date of issuance, validity and other circumstances.

3.1.2. Non-face-to-face customer due diligence

The ZPPDFT-2 provides for several options for establishing and verifying the identity of the customer and related parties on a non-face-to-face basis.

---

[6] Any document containing a photo of the bearer and issued by a government authority has the status of an official (personal) identification document in the Republic of Slovenia. The documents most commonly used are the identity card, the passport, the border pass, the driving licence, the firearms licence and the certificate of competence for operators of pleasure craft. Source: https://www.gov.si/teme/osebni-dokumenti/

[7] Opinion issued by the FIU of 20 December 2016: Establishing and verifying the identity of foreign nationals. Source: https://www.gov.si/assets/organi-v-sestavi/UPPD/Dokumenti/Mnenja/Pregled-stranke/ugotavljanje_in_preverjanje_istovetnosti_tujcev.pdf

It is important that the obliged entity assesses whether establishing and verifying the customer's identity on a non-face-to-face basis poses an increased risk (assessment of a new or existing distribution channel within the framework of the OERA), and on the basis of the assessment takes appropriate measures to mitigate the risk that the customer, the statutory representative or the authorised representative is not who they claim to be. The measures that employees must take in individual approaches to identification on a non-face-to-face basis are defined by the obliged entity in its policies, controls and procedures.

3.1.2.1. Identification in the case of insignificant risk

Under certain conditions the ZPPDFT-2 allows the obliged entity to establish and verify the identity of customers, statutory representatives or authorised representatives from a **copy of an official personal identification document** that the aforementioned persons submit to the obliged entity in **paper or digital form**.

This method of identification is only allowed when an **insignificant risk** has been determined on the basis of the CRA, and the obliged entity is also required to take **measures to manage the risks inherent in non-face-to-face transactions**. These measures should focus in particular on verifying the reliability of the submitted copy of the personal identification document, and on verifying whether it is the person being claimed, for example:

- in cases when the official document was issued with a machine-readable inscription (e.g. the bottom two lines in a passport), the algorithm used for generating the number of the original document is complete;
- in the visual image there is no discernible attempt to alter personal data;
- the specifications from the copy of the document are valid and acceptable, in particular the type, the size of the characters and the structure of the document as proceeds from official databases such as PRADO;[8]
- the photograph or copy of the personal identification document used in the submitted copy meets sufficient quality criteria to allow its future use (e.g. it allows for verification in the PRADO database);
- the customer, the statutory representative or the authorised representative is a publicly known person and the copy of the personal identification document matches the public data on that person (e.g. data from the AJPES records, commercial databases or media, where the credibility and reliability of the source needs to be taken into account in the assessment);
- in addition to the copy of the official personal identification document, the obliged entity also requires a photograph of the person together with the official personal identification document;
- in addition to the copy of the official personal identification document, the obliged entity also requires other (official) documents that confirm the statements of the customer, the statutory representative or the authorised representative (e.g. an electricity bill or utilities bill for the domicile or temporary address of the customer, statutory representative or authorised representative).

The obliged entity uses the proposed risk management measures to the extent necessary with regard to the risks identified in connection with this method of non-face-to-face identification. The obliged entity may also use other measures that it assesses to be suitable for risk management in non-face-to-face identification in the case of insignificant risk.

[8] Available at https://www.consilium.europa.eu/prado/sl/prado-start-page.html

3.1.2.2. Electronic means of identification

The obliged entity may establish and verify the identity of a natural person (i.e. the customer, the statutory representative or the authorised representative) on the basis of an electronic means of identification with a high level of reliability or on the basis of other approaches to electronic identification for access to electronic services with a high level of reliability in accordance with the regulations governing electronic identification and trust services (Article 33 of the ZPPDFT-2).

3.1.2.3. Video-based electronic identification

The establishment and verification of the identity of the customer, the statutory representative or the authorised representative may also be undertaken by means of video-based electronic identification. The ZPPDFT-2 cites the conditions that need to be met for this method of non-face-to-face identification to be used:

- increased ML/TF risk has not been identified: video-based electronic identification may only be used when low risk or medium risk has been identified on the basis of the CRA;
- the official personal identification document must feature a photograph in which the face is clearly identifiable and on which the person's name and date of birth at a minimum are cited;
- the customer, the statutory representative or the authorised representative has a domicile or registered office in a Member State or a third country that has put in place an effective AML/CFT system (the obliged entity identifies such countries and geographical regions within the framework of its own list of geographical regions as defined in Section *2.3.1.2 Country risk);*
- the customer, the statutory representative or the authorised representative does not have a domicile or registered office in countries on the list of high-risk third countries or the list of increased-risk countries;
- after entering into the business relationship the obliged entity must provide for in-depth transaction monitoring for a period of six months (e.g. daily, monthly), then monitors the customer's transactions in accordance with the CRA (*see Section 4.1 Transaction monitoring*);
- the video-based electronic means of identification must meet the minimum technical requirements prescribed in the applicable Rulebook on technical requirements for video-based electronic identification devices.[9]

3.1.2.4. Other methods

The ZPPDFT-2 introduces the possibility of establishing and verifying the identity of the customer, the statutory representative or the authorised representative through **other appropriately secure non-face-to-face administrative or electronic procedures and means of identification**. The law allows obliged entities to conduct customer due diligence by means of new technologies that already exist on the market or are yet to exist.

The conditions envisaged for the use of other methods of identification are the same as those for video-based electronic identification (*for more detail, see Section 3.1.2.4 Video-based electronic identification*). When using other methods of identification the obliged entity will have to take account of the minimum technical requirements defined in the rulebook issued pursuant to the fifth paragraph of Article 34 of the ZPPDFT-2.

Notwithstanding the above, during the use of new technologies for the purposes of establishing and verifying the identity of persons it is essential that the obliged entity assesses:

[9] The regulation currently in force is the Rulebook on technical requirements for video-based electronic identification devices (Official Gazette of the Republic of Slovenia, No. 32/18).

- the extent to which the use of innovative technological solutions can address, or might exacerbate, the ML/TF risks, in particular in non-face to face situations;
- whether the new technology poses a security risk, in particular whether the innovative solution may be unsuitable or unreliable or could be tampered with;
- qualitative risks, i.e. whether the sources of information used for verification purposes are sufficiently independent and reliable and therefore comply with national or supranational legal requirements (e.g. rules regarding the mandatory elements of passports), and also whether the extent and method of identity verification provided by the innovative solution is commensurate with the level of ML/TF risk according to the CRA methodology;
- legal risks, in particular the risk that the technological solution provider does not comply with applicable data protection legislation; and
- impersonation fraud risks (i.e. the customer is not who they claim to be) or the risk that the person is not a real person.

3.1.2.5. Identification in the case of correspondent relations

When the customer is a **bank or another credit institution**, the ZPPDFT-2 allows obliged entities referred to in points 1 and 2 of Section 1.2 Scope of application to establish and verify the identity of its statutory representatives and authorised representatives using the method **normally used in international banking relationships**. This means that their identity is established on the basis of publicly available information about the bank or other credit institution, or on the basis of documentation submitted by the customer and verified by means of credible sources (e.g. Bankers Almanac, SWIFT KYC Registry).

The aforementioned method of identification is not allowed when the bank or other similar credit institution is established in a country on the list of high-risk third countries.

3.1.2.6. Due diligence via third parties

Under the conditions set out in the ZPPDFT-2, the obliged entity may **entrust customer due diligence to certain third parties**. The set of third parties that may conduct due diligence (e.g. banks, insurance corporations and payment institutions in EU Member States, a notary public established in the Republic of Slovenia) and the set of third parties that may not (e.g. shell banks, third-country payment institutions) is defined in detail by the ZPPDFT-2.

In connection with the establishment and verification of the identity of the customer, the statutory representative or the authorised representative, it is important that the third party verifies the identity **in person** or using an **electronic means of identification with a high level of reliability** or **other approaches to electronic identification for access to electronic services with a high level of reliability**.

3.1.2.7. Due diligence via external service provider

The obliged entity may conduct customer due diligence via an external service provider that is not deemed a third party. When commissioning the external service provider, the obliged entity acts in accordance with the requirements of the third, fourth and fifth paragraphs of Article 17 of the ZPPDFT-2.

3.2. Scope of due diligence with regard to CRA

Based on the customer risk category, the obliged entity determines the type of customer due diligence, which includes the process of obtaining information about the customer, the type of transaction monitoring, and the frequency of the review and updating of the information and documentation. Here the principle of proportionality applies, in line with which higher-risk

customers are subject to more frequent and broader-scope controls, while lower-risk customers are subject to less frequent and narrower-scope controls.

Standard due diligence is sufficient in connection with customers **assessed as posing medium ML/TF risks** on the basis of the risk criteria.

The CRA methodology must include risk criteria that will identify **customers that pose high ML/TF risks**. In these cases the obliged entity is required to conduct **enhanced due diligence** before entering into the business relationship, and later in-depth transaction monitoring.
A certain segment of customers pose **low ML/TF risks**; **simplified due diligence** is allowed in these cases.

Here it should be particularly noted that the **requirement to conduct enhanced due diligence is binding**, in contrast to the **option of conducting simplified due diligence, which is a matter to be decided by the obliged entity**.

In accordance with the ZPPDFT-2 and the guidelines, obliged entities define **measures of standard, simplified and enhanced due diligence in detail in their internal policies and bylaws**.

3.2.1. Standard due diligence

In customer due diligence, the obliged entity reliably determines and verifies the customer's identity, and establishes the purpose of the transaction or the intended nature of the business relationship, thereby mitigating the risk of doing business with an unknown customer who might try to use the obliged entity for ML/TF.

The following measures are carried out by the obliged entity within the framework of standard due diligence:

- it determines and verifies the **customer's identity** on the basis of the information and documents required by law;
- it verifies that each person acting on behalf of the customer holds the **right of representation or an authorisation** from the customer, and establishes and verifies the identity or the statutory representative or authorised representative;
- it identifies and obtains the information about the **BO** required by law;
- it obtains information about the **purpose and intended nature** of the business relationship or transaction;
- it determines and verifies the **political exposure of the customer and the BO**.

When the obliged entity is conducting standard due diligence on a customer on the basis of the CRA and in accordance with its CRA methodology, it **monitors the customer's transactions on a half-yearly basis**, and **reviews and updates the information and documentation about the customer every two to three years**.

3.2.2. Simplified due diligence

When the obliged entity assesses on the basis of the CRA and in accordance with its CRA methodology that simplified due diligence may be conducted on a customer, it is still required to carry out all measures prescribed under customer due diligence (including verifying whether the customer or the BO is a PEP), except that the measures may be slightly simplified, which allows for the following:

- a **reduced set of information** about the customer, the statutory representative, the authorised representative and the BO;

- **simplified verification of the identity of the customer, statutory representative or authorised representative** by viewing a copy of an official personal identification document that the aforementioned persons submit to the obliged entity in paper or digital form (*for more details, see Section 3.1.2.1 Identification in case of insignificant risk*), and in the case of legal persons by viewing the original or a certified copy of documentation from a relevant register or by viewing the register directly;
- **simplified review of the BO**: the obliged entity obtains the information about the BO required by law on the basis of a declaration by the statutory representative or the authorised representative, and not by viewing the original or a certified copy of documentation from a relevant register or by viewing the register directly;
- **information on the purpose and intended nature of the business relationship** or the purpose of the transaction is only required if it is not evident from the business relationship or transaction itself (*e.g. purpose-specific loans, deposits*);
- **less frequent transaction monitoring** of the customer **(annual)** and a **longer period for reviewing and updating information and documentation (3 to 5 years)**.

In the event of any doubt about the credibility and adequacy of the information obtained about the customer or the customer's BO or if there are grounds for suspecting ML/TF in connection with the transaction, the customer, the funds or the assets, there is a need to employ standard or even enhanced due diligence, and to report the transaction to the FIU in the case of suspected ML/TF.

3.2.3. Enhanced due diligence

In addition to the measures prescribed within the framework of standard due diligence, enhanced due diligence requires the obliged entity to carry out additional measures for the purpose of improved management of the risks posed by customers, transactions and business relationships.

The obliged entity's CRA methodology should ensure that enhanced due diligence is always conducted in cases set out by the **ZPPDFT-2**:

- a **direct account relationship** with a bank or another similar credit institution established in a third country;
- a business relationship or transaction with a **PEP** (*details in Section 3.2.3.1 Features of enhanced due diligence for PEPs*);
- a business relationship or transaction with a **customer with links to a country that is on the list of high-risk third countries** (*details in Section 3.2.3.2 Features of enhanced due diligence for customers linked to the list of high-risk third countries*);
- a business relationship in which the obliged entity has identified **increased ML/TF risk on the basis of the risk assessment**.

In cases where the ZPPDFT-2 requires enhanced due diligence, the obliged entity takes account of the enhanced due diligence measures laid down in the act. When the obliged entity identifies increased or high ML/TF risks on the basis of its risk assessment, it carries out one or more of the following enhanced due diligence measures:

- **additional review of information about the customer's business activities**: verifying whether the legal person's business activities reasonably match the business activities of suppliers and customers, evidence of the employment of a customer who is a natural person; additional review of the reputation of the customer and related parties (*e.g. media information*);
- **additional review of information about the purpose and intended nature of the business relationship**: in particular the scale and purpose of cash transactions and the destination of cross-border transactions;
- **additional review of information about the reasons for the intended or executed transaction**: especially in the case of unusual transactions;
- collection of **information on the source of funds and source of wealth of the customer and BO and information on the source of funds and wealth that have been or will be the subject of a business relationship or transaction**: more detailed information and evidence on the source of financing is obtained for newly established legal persons, and statements on the source of funds and general wealth of the person in question are verified for natural persons (*e.g. with regard to his/her employment, general knowledge about the customer*);
- **checking the credibility of information and documentation obtained from external sources:** checking information in the register of BOs (accessible at AJPES); checking the validity of the personal identity document in the public register of authentic identity and travel documents online (PRADO);[10]
- **written approval** of the business relationship (new or continuation of existing one) by a **responsible person in a senior management function**;
- **assessment** of the compliance of the business relationship **by the AML/CFT officer** (*in exceptional cases when professional judgement and assessment of ML/TF risks are required: e.g. entering into business relationships with customers on lists of restrictive measures, transaction monitoring for PEPs*);
- **more frequent transaction monitoring (monthly)**; and
- a **shorter period for reviewing and updating** information and documentation about the customer **(one to two years)**.

In accordance with the internal customer acceptance policy, the obliged entity defines which of the aforementioned enhanced due diligence measures it will carry out with regard to business with high-risk customers, where **more frequent transaction monitoring and a shorter period**

[10] Available at https://www.consilium.europa.eu/prado/sl/prado-start-page.html.

of reviewing and updating information and documentation about the customer[11] are mandatory measures in enhanced due diligence (unless stipulated otherwise by the ZPPDFT-2 and the guidelines, *e.g. features with regard to PEPs and customers with links to countries on the list of high-risk third countries*).

For the effective management of ML/TF risks, in addition to the measures cited above, the obliged entity may also carry out other enhanced due diligence measures as laid down in their own policies, controls and procedures.

3.2.3.1. Features of enhanced due diligence for PEPs

PEPs pose a high ML/TF risk because of the risk that they will use the power and influence deriving from their public function for their personal gain, or for the advantage of family members, associates, or other legal and natural persons. For this reason the ZPPDFT-2 defines PEPs as natural persons on whom obliged entities are always required to conduct **enhanced due diligence measures**, which in addition to standard due diligence measures also includes:

- the collection of information about the source of funds and wealth that are or will be the subject of the business relationship or transaction;
- written approval from a superior responsible person in a senior management function before a new business relationship is entered into;
- particularly diligent transaction monitoring and ongoing monitoring of the customer's other business activities.

Review of political exposure

Under Article 66 of the ZPPDFT-2 obliged entities are required to define the procedure by which they determine whether a customer (natural person) or the BO of a legal person is a PEP. The Slovenian government regularly publishes a list of functions deemed to be prominent public positions,[12] and this can aid obliged entities in determining the political exposure of customers and BOs. The obliged entity ensures that the procedure for determining political exposure is recorded (e.g. storage of PEP questionnaires, evidence of reviewing PEPs). Obliged entities put in place a procedure for automatically determining the political exposure of customers and BOs using IT support and commercial PEP databases (e.g. Dow Jones WatchList, World Check). Where the sectoral guidelines allow (*details in Section 6 Sectoral guidelines for individual obliged entities*), obliged entities may carry out the procedure of reviewing PEPs without IT support based on a statement by the customer or statutory representative (i.e. PEP questionnaire).

The procedure for determining a PEP is required before the business relationship is entered into, and during the business relationship, or prior to the conclusion of an occasional transaction. Obliged entities are required to review the political exposure of customers and BOs **when information that could lead to political exposure is received** (*e.g. elections to parliament, information about the appointment of a new supervisory board at an undertaking under government ownership*), and no later than during the review and updating of information and documentation obtained about the customer (in accordance with the CRA methodology and the customer risk category). Obliged entities that have put automatic review of PEP status in place review their

[11] Article 54 of the ZPPDFT-2 stipulates that the obliged entity must conduct ongoing monitoring of the business activities that a customer pursues with it for the duration of the business relationship. The sixth paragraph of the aforementioned article stipulates that the obliged entity must ensure that the scope and frequency of the measures for the ongoing monitoring of the customer's business activities are tailored to the ML/TF risks that the obliged entity is exposed to when executing a particular transaction or when doing business with the customer. This risk is determined by the obliged entity on the basis of a risk assessment.

[12] The currently valid list is published in the Decree on the exact functions which qualify as prominent public functions in the Republic of Slovenia (Official Gazette of the Republic of Slovenia, No 164/20).

existing customers during any changes to relevant information and any changes to PEP information in commercial databases.

Irrespective of the procedure for reviewing PEP status (automatically on the basis of commercial databases, or via a PEP questionnaire), the obliged entity must ensure that information on political exposure with regard to the customer or the related party obtained from other sources is taken into account in the CRA.

Not all PEPs pose the same ML/TF risks; therefore applying the same treatment to all PEPs would be disproportionate. Guidance is given below to help distinguish between lower- and higher-risk PEPs.

New business relationship

If when entering into a new business relationship with a customer (**natural person**) the obliged entity determines that the **customer is a PEP**, it is required to carry out enhanced due diligence measures as cited by the ZPPDFT-2:

- collecting information about the source of funds and wealth that are or will be the subject of the business relationship or transaction with the customer;
- obtaining written approval from a superior responsible person in a senior management function;
- placing the customer in a customer risk category that is the same as or comparable to the customer risk category of high risk as set out by the obliged entity's methodology; and
- monitoring their business operations monthly.

If when entering into a business relationship with a customer (natural person) the obliged entity determines that the customer's statutory representative or authorised representative is a PEP (domestic or foreign PEP), the obliged entity takes account of the identified information as one of the customer-related risk criteria with a level of increased risk, and conducts the CRA in conjunction with other risk criteria, placing the customer into the relevant customer risk category. The scope of customer due diligence and the frequency of transaction monitoring are carried out in accordance with the customer risk category.

When entering into business relationships with **legal persons**, the obliged entity must also check any **political exposure of the customer's BO**. The scope of the enhanced due diligence applying to PEPs in these cases relates to the **legal person**, whereby the obliged entity must take account of the following features with regard to enhanced due diligence measures:

a) if the obliged entity concludes a business relationship with an entity for which the **second paragraph of Article 43 of the ZPPDFT-2 does not require the customer's BO to be identified** (the Republic of Slovenia, self-governing local communities and their core sections, the government, ministries, affiliated bodies, government services, administrative units and other state bodies, Banka Slovenije, public agencies, public institutes not co-founded by natural persons or legal person of private law, public funds), there is no need to review the political exposure of the BO for such entity;

b) if an obliged entity concludes a business relationship with a **legal person or an entity where the BO has been identified in accordance with the fifth paragraph of Article 42 or first paragraph of Article 43 of the ZPPDFT-2** (*e.g. the president of the management board of a legal person under majority government ownership, president of a political party)*:
    - in determining the *customer risk category*, account is taken of the information about PEP status as one of the customer risk criteria with a level of increased risk, and the

CRA is conducted in conjunction with other risk criteria, placing the customer into the relevant customer risk category;
- *the scope of customer due diligence and transaction monitoring* are carried out in accordance with the customer risk category: simplified, standard or enhanced due diligence, monthly, half-yearly, annual;
- as *an additional measure* the obliged entity obtains information on the source of funds that will be the subject of the business relationship or transaction with the customer, written approval from a superior responsible person in a senior management function, and the AML/CFT officer's opinion with regard to the appropriateness of the customer risk category;

c) if the obliged entity is entering into a business relationship with a **legal person whose BO is a PEP:**
   - *in determining the customer risk category* it should place the customer in the customer risk category that is the same as or comparable to the customer risk category of high risk as set out by the obliged entity's methodology;
   - it should conduct enhanced customer due diligence (Section 3.2.3 Enhanced due diligence) and monitor its transactions monthly (Section 4.1 Transaction monitoring);
   - *as an additional measure* the obliged entity obtains information on the source of funds and wealth that will be the subject of the business relationship or transaction with the customer (i.e. a legal person), and written approval from a superior responsible person in a senior management function;

d) if the obliged entity is entering into a business relationship with a **legal person whose BO is a foreign PEP:**
   - *in determining the customer risk category* it should place the customer in the customer risk category that is the same as or comparable to the customer risk category of high risk as set out by the obliged entity's methodology;
   - it should conduct enhanced customer due diligence (Section 3.2.3 Enhanced due diligence) and monitor its transactions monthly (Section 4.1 Transaction monitoring);
   - *as an additional measure* the obliged entity obtains information on the source of funds and wealth that will be the subject of the business relationship or transaction with the customer (i.e. a legal person), written approval from a superior responsible person in a senior management function, and the AML/CFT officer's opinion providing an assessment whether the reasons for which the foreign PEP (*see Section 1.3 Definition of terms*) is entering into a business relationship via the legal person and outside the country in which they hold a political function pose potential ML/TF risks.

The enhanced due diligence measures as described for PEPs in this section of the guidelines (New business relationship) apply *mutatis mutandis* to the execution of occasional transactions.

Collection of information about the source of funds and wealth of PEPs

With regard to the scope and method of obtaining information about the source of funds and wealth that are or will be the subject of the business relationship, the **obliged entity takes account of the risk posed by the PEP** or the risk identified by the CRA. Information about the **source of funds and wealth** is obtained from public records or documents and other documentation submitted to the obliged entity by the customer (*e.g. the payroll, decision on inheritance of monetary assets that will be the subject of the business relationship, contract on the sale for instance of a car, real estate, securities, virtual currencies and other comparable evidence*). If this is not possible, information about the source of funds and wealth is collected directly via

written statement by the customer.[13] If the risk associated with PEPs is extremely high, obliged entities should check the source of funds and wealth on the basis of reliable and independent data, documents or information.

Existing customer

When an existing customer (natural person) or the BO of a legal person becomes a PEP during the business relationship (*for details see Review of political exposure*), the obliged entity knows the customer and the customer's transactions, and therefore carries out enhanced due diligence measures as follows:

- **information about the source of funds and wealth is obtained on the basis of existing and known facts about the customer**, and there is no need to request it directly from the customer;
- the continuation of the business relationship with a customer who has become a PEP is **approved in writing by the superior responsible person in a senior management function**;
- the customer is placed in the relevant customer risk category and the **PEP's transactions are monitored**, as described in detail below (see *Transaction monitoring of PEPs*).

Transaction monitoring of PEPs

The fact that the customer or BO is a PEP affects the CRA and consequently also the frequency of transaction monitoring. In cases where based on the CRA the obliged entity places the customer in a category that is the same as or comparable to the customer risk category of high risk as set out by the obliged entity's methodology, it must monitor the customer's transactions monthly.

If the obliged entity judges that the transactions of a customer **do not deviate from the stated purpose and scale of transactions**, or the **obliged entity assesses that the customer's transactions pose no ML/TF risks, it may reduce the frequency of transaction monitoring**, provided that all of the following conditions are met:

- the customer's transactions do not deviate for more than one year following the beginning of enhanced monitoring;
- the other risk criteria are assessed as low-risk or medium-risk;
- the obliged entity has provided for IT support that will immediately warn the responsible employee at the obliged entity of any deviations from the purpose and scale of transactions;
- an opinion has been obtained from the AML/CFT officer; and
- the decision has been approved by the superior responsible person in a senior management function.

The frequency of transaction monitoring may be reduced to **annual monitoring** if the customer was assessed as a low risk before acquiring PEP status, or to **half-yearly monitoring** if the customer was assessed as a medium risk before acquiring PEP status.

A customer that is a PEP or whose BO is a PEP nevertheless **remains in a customer risk category that is the same as or comparable to the customer risk category of high risk as set out by the methodology of the obliged entity**. Given the high risk, it is also necessary to provide for the procedure of reviewing and updating the information and documentation obtained about the customer with a frequency of at least every one to two years (*see Section 4.2 Review and updating of information and documents*).

---

[13] Similarly, the FIU stated the following in an opinion published on its website (in Slovene) at
- https://www.gov.si/assets/organi-v-sestavi/UPPD/Dokumenti/Mnenja/Politicno-izpostavljene-osebe/politicno_izpostavljene_osebe.pdf, and
- https://www.gov.si/assets/organi-v-sestavi/UPPD/Dokumenti/Mnenja/Politicno-izpostavljene-osebe/PEP_usmeritve.pdf.

3.2.3.2.Features of enhanced due diligence of customers linked to the list of high-risk third countries

In accordance with the AMLD, the European Commission adopts a delegated act defining high-risk third countries that have strategic deficiencies in AML/CFT. The list is published by the FIU on its website[14] i.e. the list of high-risk third countries (*for details see Section 1.3 Definition of terms*).

Reviewing customers linked to the list of high-risk third countries

Under the ZPPDFT-2 the obliged entity is required to carry out enhanced due diligence measures when the customer has links with a country on the list of high-risk third countries.

A customer has links with a high-risk third country when:

- they are a national of a country that is on the list of high-risk third countries;
- they have a registered office or they have a domicile or temporary residence in a country that is on the list of high-risk third countries;
- their statutory representative, authorised representative or BO is a national of a country that is on the list of high-risk third countries;
- the customer's statutory representative, authorised representative or BO has a domicile or temporary residence in a country that is on the list of high-risk third countries.

The review is conducted before the business relationship is entered into, and during the business relationship, and encompasses:

- additional review of information about the customer's business activities;
- additional review of the information about the purpose and intended nature of the transactions, and information about the reasons for the intended or executed transaction;
- collection of information about the customer's source of funds and wealth (legal or natural person) and the BO of the legal person;
- collection of information about the source of funds and wealth that are or will be the subject of the business relationship;
- approval of the business relationship by a responsible person in a senior management function;
- more frequent transaction monitoring (monthly); and
- a shorter period for reviewing and updating information and documentation about the customer (1-2 years).

The obliged entity may itself obtain information about the customer's source of funds and wealth (legal or natural person) and the BO of the legal person, as well as information on the source of funds and wealth that are or will be the subject of the business relationship, if it has access to information clearly indicating the source of funds and wealth, or obtain such information from the customer.

If when entering into a business relationship with a legal or natural person that has a **domicile or temporary residence or registered office in a country on the list of high-risk third countries** (or a related party [statutory representative, authorised representative, BO] has a domicile or temporary residence in such a country), the obliged entity must ensure that the **customer is placed in a customer risk category that is the same as or comparable to the customer risk category of high risk as set out by the methodology of the obliged entity**.

[14] http://www.uppd.gov.si/si/javne_objave/seznam_drzav_50_clen_zppdft_1/

If the customer or the statutory representative, authorised representative or BO is a **national of a country that is on the list of high-risk third countries, the risk criterion is assessed as increased risk**, which together with the other risk criteria has an impact on the CRA (*for more detail, see Section 2.3.1.2 Country risk*).

Monitoring transactions of customers linked to the list of high-risk third countries
Under the guidelines the transactions of high-risk customers are monitored at least monthly (*for more detail, see Section 4.1 Transaction monitoring*).

If the obliged entity judges that the transactions of a customer who has a domicile, temporary residence or registered office in a country on the list of high-risk third countries **do not deviate from the stated purpose and scale of transactions**, or the **obliged entity assesses that the customer's transactions pose no ML/TF risks, it may reduce the frequency of transaction monitoring**, provided that all of the following conditions are met:

- the customer's transactions do not deviate for more than one year following the beginning of enhanced monitoring;
- the other risk criteria are assessed as low-risk or medium-risk;
- the obliged entity has provided for IT support that will immediately warn the responsible employee at the obliged entity of any deviations from the purpose and scale of transactions;
- an opinion has been obtained from the AML/CFT officer; and
- the decision has been approved by the superior responsible person in a senior management function.

A customer that has a domicile or temporary residence or a registered office in a country on the list of high-risk third countries nevertheless **remains in a customer risk category that is the same as or comparable to the customer risk category of high risk as set out by the methodology of the obliged entity**. Given the high risk, it is also necessary to provide for the procedure of reviewing and updating the information and documentation obtained about the customer with a frequency of at least every one to two years (*see Section 4.2 Review and updating of information and documentation*).

Reviewing transactions linked to the list of high-risk third countries
The ZPPDFT-2 stipulates that the obliged entity is also required to carry out enhanced due diligence measures when a transaction has links with a country on the list of high-risk third countries, and in so doing must obtain information about the reasons for the intended or executed transaction.

Transactions are related to countries on the list of high-risk third countries when:

- they are made to payment accounts in countries on the list of high-risk third countries or
- they are made to payment accounts of natural and legal persons with a registered office, domicile or temporary residence in countries on the list of high-risk third countries.

A transaction may be executed within the framework of a business relationship that has been entered into, or as an occasional transaction.

Transactions within the framework of a business relationship that has been entered into:

- within the framework of the transaction monitoring of the customer, the obliged entity judges whether transactions linked with countries on the list of high-risk third countries accord with the purpose, nature and scale of the customer's transactions and, in the event of any deviation being identified, obtains additional evidence (*e.g. invoices, delivery notes,*

contracts) based on which it will be possible to establish the reasons for the intended or executed transactions linked with such countries;
- here the obliged entity must report to the FIU any transaction that exceeds EUR 15,000, in accordance with Article 75 of the ZPPDFT-2;
- in the event of the identification of suspicious conduct on the part of a customer in connection with transactions linked with countries on the list of high-risk third countries, the obliged entity assigns the customer to a customer risk category that is the same as or comparable to the customer risk category of high risk as set out by the methodology of the obliged entity, and assesses whether the suspected ML/TF should be reported to the FIU.

Occasional transactions

The ZPPDFT-2 defines an occasional transaction as any transaction executed by a person who has not entered into a business relationship with the obliged entity. If an occasional transaction entails the transfer of funds in excess of EUR 1,000, the law requires customer due diligence to be conducted.

If an occasional transaction for which the ZPPDFT-2 requires customer due diligence is ordered by a person linked with a country on the list of high-risk third countries, or the transaction is executed into the accounts of legal or natural persons in a country on the list of high-risk third countries or into the accounts of legal and natural persons that have a registered office or domicile or temporary residence in a country on the list of high-risk third countries, the obliged entity is required to carry out the following enhanced due diligence measures:
- obtain information on the reason for the intended occasional transaction;
- obtain information about the source of funds and wealth of the legal or natural person and/or the BO of the legal person;
- obtain information about the source of funds and wealth that are or will be the subject of the transaction.

Payment transactions

As an additional measure of enhanced due diligence in the case of transactions linked with countries on the list of high-risk third countries (executed either within the framework of a business relationship or as an occasional transaction), obliged entities that are authorised to provide payment services ensure that transactions are always accompanied by information about the purpose of the transaction.

4. Transaction monitoring

4.1. Frequency of transaction monitoring

Transaction monitoring differs with regard to customer risk category: under the ZPPDFT-2 the obliged entity is required to verify that the customer's transactions comply with the purpose and intended nature of the transactions, and to review any deviations from usual transactions.

The frequency of transaction monitoring for a particular customer depends on the CRA: more frequent monitoring is required for higher-risk customers, with less frequent monitoring for lower-risk customers (the principle of proportionality). Under the guidelines it is necessary to conduct transaction monitoring as follows:

- **annually** for **low-risk customers**,
- **half-yearly** for **medium-risk customers**,
- **monthly** for **high-risk customers**.

The **customer risk category** and the corresponding frequency of transaction monitoring do not affect the obliged entity's requirements with regard to monitoring individual high-risk transactions: the obliged entity must provide for the monitoring of at least the following high-risk transactions **on a daily basis** (irrespective of the CRA executing the transaction):

- transactions referred to in Article 75 of the ZPPDFT-2, irrespective of whether the customer appears in the role of payer or payee;
- transactions in a previously dormant account;
- other high-risk transactions, if their characteristics indicate the need for daily monitoring.

With regard to the risk criteria deriving from the customer's transactions themselves, the obliged entity must also provide for the **regular updating of the CRA**. Irrespective of the envisaged period for repeating customer due diligence, the obliged entity must update the CRA whenever it identifies any suspected ML/TF in connection with the customer or a transaction, and whenever it establishes during the customer's transactions that a risk criterion is classed as a high risk in line with its CRA methodology (*e.g. the customer is a PEP, a report of suspected ML/TF risks to the FIU*).

To ensure effective risk management in the area of AML/CFT, obliged entities are recommended to put in place adequate IT support for transaction monitoring. In accordance with the principle of proportionality, the aforementioned recommendation is regulated differently for individual obliged entities (*for more detail, see Section 6 Sectoral guidelines for individual obliged entities*).

4.2. Review and updating of information and documentation

Under the ZPPDFT-2 obliged entities are required to review and update the information and documentation obtained about the customer, whereby the obliged entity tailors the scope and frequency to the ML/TF risks identified on the basis of the CRA, or undertakes review and updating no more than five years after the last review of the customer if the customer has executed at least one transaction with the obliged entity in the last 12 months. This provision of the law requires the obliged entity to check whether all the information and documentation received when the business relationship was entered into with the customer or during the business relationship is still adequate, including a **review of whether the customer is doing business in line with the purpose, the intended nature and the scale of the transactions**. Obliged entities that have not put in place a procedure for automatically determining the political exposure of customers and BOs should also check, as part of periodic due diligence, whether the **customer or BO has become a PEP**. The obliged entity keeps an appropriate record of the repeated customer due diligence and in light of the checks updates the information and CRA as necessary.

In so doing the obliged entity applies a risk-based approach, which means that more frequent updating of the information and documentation obtained about the customer must be put in place for customers that pose a higher ML/TF risk.

The obliged entity reviews and updates the existing information and documentation about the customer:

- **every three to five years** for a **low-risk** customer;
- **every two to three years** for a **medium-risk** customer;
- **every one to two years** for a **high-risk** customer.

Obliged entities are recommended to **put in place IT support that will warn employees of the need to review and update the information and documentation about the customer** and will also include an audit trail with regard to the due diligence conducted. In accordance with the principle of proportionality, the aforementioned recommendation is regulated differently for individual obliged entities (*for more detail, see Section 6 Sectoral guidelines for individual obliged entities*).

The **customer is not required to be present in person** when the information and documentation about the customer are being updated. The obliged entity may obtain information and documentation on the basis of credible evidence submitted by the customer (*e.g. via electronic identification means, online banking, email, ordinary mail, via a third party or agent/intermediary*).

If the customer fails to submit the required information and documentation when called on to do so by the obliged entity, or the information cannot be updated because the customer is failing to respond, **the obliged entity restricts the transactions of a customer assessed as an increased risk or a high risk**, as follows:

- **it does not enter into any additional business relationship** until the customer has submitted the information and documentation required for the update;
- **it does not execute transactions referred to in point 2 of the first paragraph of Article 22 of the ZPPDFT-2 that require customer due diligence in accordance with the ZPPDFT-2.**

The obliged entity may also apply the aforementioned measures to customers that it assesses as low-risk or medium-risk, if it determines via the risk-based approach that such a measure is necessary.

The products and services that the obliged entity offers on the basis of a business relationship entered into previously are not subject to restrictions; transactions for which customer due diligence is not required under the ZPPDFT-2 are also not subject to restrictions.[15]

In any case, the **customer's lack of response to the obliged entity's call to submit the information and documentation required to carry out the updating required by law needs to be assessed from the perspective of ML/TF risks**, and within this framework there is also a need to judge the possible reasons for suspecting ML/TF and to report suspicious transactions to the FIU, and the possibility of continuing the business relationship with the customer.

In the case of a **dormant account**, there is no need for transaction monitoring or the review and updating of the information and documentation about the customer. However the obliged entity must ensure that in the event of the reactivation of the account (a transaction is executed again after a period of more than 12 months), the customer's activities are immediately flagged, and

[15] I.e. transactions not covered by point 2 of the first paragraph of Article 22 of the ZPPDFT-2.

customer due diligence is repeated, which also includes the updating of the previously obtained information and documentation as necessary. The reactivation of a dormant account needs to be taken into account in the CRA as one of the product/service/transaction risk criteria.

5. Customer acceptance policy and prohibited transactions

5.1. Customer acceptance policy

The obliged entity formulates and updates its customer acceptance policy on the basis of the OERA; this document sets out its **intentions with regard to doing business with customers covered by individual CRAs** (*see Section 6 Sectoral guidelines for individual obliged entities*).

The aforementioned policy combines the **obliged entity's business strategy** and **risk management in the area of AML/CFT**. If the obliged entity sees its business opportunities in higher-risk customers, products, services, transactions or distribution channels, it must strengthen its control environment as appropriate for the effective management of the increased risks posed by such customers, products, services and transactions (*e.g. enforcement of additional controls, increase in the number of employees in the AML/CFT department, application of the four-eyes principle*), and conversely, if the obliged entity's business stance poses lower ML/TF risks, a control environment is allowed that is tailored to the lower risks that the obliged entity is willing to take up.

The customer acceptance policy must also set out the circumstances in which the obliged entity will not enter into a new business relationship or will terminate an existing business relationship on account of the excessive risk that the obliged entity's system could be misused for ML/TF.

Financial inclusion and risk reduction (de-risking)

The obliged entity must ensure that in adopting its customer acceptance policy it is not unjustifiably preventing access to financial services for legitimate customers (e.g. PEPs and their close family members, asylum seekers, non-residents, humanitarian organisations, entities in certain commercial activities such as the defence sector).

De-risking relates to the decision of the obliged entity to no longer offer services to certain categories of customers associated with a higher ML/TF risk. Such actions are not in accordance with a risk-based approach, since the risk associated with individual customers, transactions and business relationships can differ within a single category, and rejection or termination of a business relationship with entire categories of customers deemed to pose a higher ML/TF risk can therefore be unjustified. In the customer acceptance policy the obliged entity should therefore seek a balance between financial inclusion and the need to mitigate ML/TF risk.

An obliged entity that identifies a group or category of customers for which it determines a higher level of risk, should examine the possibilities for managing ML/TF risk and (i) either adapt the scope and frequency of transaction monitoring or (ii) offer only basic financial products and services that limit the possibility of users misusing these products and services for the purpose of ML/TF. Such basic products and services can additionally help obliged entities to recognise unusual transactions or patterns of transactions, including the unintended use of a product, but it is important here for all the restrictions to be proportionate and for the access of customers to financial products and services not to be excessively or unnecessarily limited.[16]

[16] See e.g. the EBA opinion on the application of customer due diligence measures to customers who are asylum seekers from higher-risk third countries or territories, EBA-OP-2016-07 (https://www.eba.europa.eu/eba-publishes-opinion-on-the-application-of-customer-due-diligence-measures-to-customers-who-are-asylum-seekers-from-higher-risk-third-countries-or-te), and the EBA appeal to ensure easier access to payment accounts for refugees from Ukraine (https://www.eba.europa.eu/eba-calls-financial-institutions-ensure-compliance-sanctions-against-russia-following-invasion).

5.2. Prohibited transactions

Article 71 of the ZPPDFT-2 prohibits the **use of anonymous products** that could directly or indirectly allow for the concealment of the customer's identity, which obliged entities take into account when assessing the risk of a new product or service.

The ZPPDFT-2 also explicitly prohibits transactions with customers who prove their ownership of a legal person or a similar entity of foreign law on the basis of **bearer shares** whose **traceability is not facilitated via KDD** or a similar register or via trading accounts, and that **cannot be established on the basis of other business documentation**.

If the customer submits credible evidence that proves the ownership of the bearer shares (*e.g. a contract, notarial protocol or share register of a foreign authority*), a business relationship may be entered into with the customer, but it is necessary to treat the customer as a high risk (a customer risk category that is the same as or comparable to the customer risk category of high risk as set out by the obliged entity's methodology) and consequently to carry out enhanced due diligence measures before entering into the business relationship and during it. An exception is made for undertakings whose records of holders of bearer shares are administered by KDD. In light of the regular updating of this data and the oversight of changes in the data on shareholders, the obliged entity may treat this risk criterion as a medium risk.

The law also prohibits obliged entities from entering into business relationships with **shell banks or banks doing business with shell banks**. Before entering into a business relationship or exchanging a key, obliged entities that have correspondent or direct account relations with banks are required to verify whether the bank is acting as a shell bank or does business with banks of this type.

6. Sectoral guidelines for individual obliged entities

The sectoral guidelines are aimed at individual obliged entities for the purpose of tailoring the arrangements for certain requirements under the general guidelines, having regard for the risks identified as part of the national risk assessment and supranational risk assessment, to the following:

- **payment institutions (that are not also banks or savings banks);**
- **e-money issuers;**
- **currency exchange offices;**
- **virtual currency service providers.**

The sectoral guidelines set out requirements tailored to the attributes of individual obliged entities, and in this part deviate from the basic sections of the guidelines. With regard to the requirements that the sectoral guidelines do not regulate, the requirements of the basic sections of the guidelines apply. The sectoral guidelines do not apply to obliged entities that provide the services of individual obliged entities but are also banks, savings banks or branches of foreign banks.

When taking account of the sectoral guidelines it is important for obliged entities to tailor the AML/CFT measures to the nature and scale of their operations, and thereby in assessing risk to abide by the principle of proportionality.

6.1. Sectoral guidelines for payment institutions

This section applies to obliged entities that are payment institutions. Payment institutions should also take account of the ML/TF risk factors guidelines, especially Guideline 11: Sectoral guideline for money remitters and Guideline 18: Sectoral guideline for payment initiation service providers.

Payment institutions provide payment services for which they have obtained the relevant authorisation pursuant to the ZPlaSSIED. There are ML/TF risks inherent in the customers, and in the transactions that customers execute within the framework of a business relationship and in occasional transactions as defined by the ZPPDFT-2.

6.1.1. Risk assessment

In accordance with Article 18 of the ZPPDFT-2 and the guidelines, payment institutions draw up an OERA and CRA and implement AML/CFT measures depending on the risk identified.

In defining the risk criteria of the OERA and CRA, payment institutions should follow the guidelines, except where the sectoral guidelines provide otherwise.

Payment institutions that are classed as a micro or small enterprise in accordance with the ZGD-1 should update the **OERA** and review and update the risk criteria and **CRA** methodology **at least once every two (2) years**.

6.1.1.1. Obliged entity's risk assessment

OERA methodology

1. <u>Inherent risk</u>

In assessing inherent risk, payment institutions should take into account the following product/service/transaction risk criteria:

a) products:
   - payment accounts (*e.g. volume of transactions in resident/non-resident payment accounts*);

- payment cards or similar devices (*e.g. volume of transactions relative to the type or limit of product);*
- loans (*e.g. volume of resident/non-resident loan payments*);
- other products offered by the payment institution;

b) services:
- payments via points of sale (*e.g. number of physical points of sale in Slovenia/outside Slovenia and number of online points of sale*);
- cash transactions (*e.g. number of ATMs in Slovenia/outside Slovenia*);
- execution of money orders (*e.g. volume of received/sent remittances*);
- payment orders (*e.g. volume of payments ordered/volume of payments ordered from or into countries that are on the list of high-risk third countries*);
- other services provided by the payment institution;

c) transactions: volume of transactions in view of country risk (*e.g. volume of payment transactions or money orders from or into countries that are on the list of high-risk third countries; volume of cash transactions*).

If payment institutions have their operations arranged by individual areas, it is recommended that their inherent risk be determined by areas (*e.g. transactions with customers/users; transactions with points of sale*).

2. <u>Control environment</u>

Payment institutions assess the control environment within the framework of the areas set out in the general guidelines, except for:
- relative to the size and the organisation, payment institutions that are classed as a micro or small enterprise in accordance with the ZGD-1 are not required to assess the areas of **Reporting** and **Independent audit**;
- in cases where the AML/CFT officer and/or their deputies do not perform this function exclusively, in the area of **AML/CFT function** an assessment is made as to whether they are allowed to effectively perform the duties of the AML/CFT officer and the deputy in accordance with Article 85 of the ZPPDFT-2.

Obliged entity's measures on the basis of the OERA

The requirement under the general guidelines that the responsible employees at the obliged entity (the AML/CFT officer, the responsible management board members, or other employees) present the results of the OERA to the persons responsible for individual business lines and to the internal audit department (point 3 of the first paragraph of Section 2.2.2 Obliged entity's measures on the basis of the OERA) is not binding on payment institutions. Notwithstanding the above, this measure is recommended for payment institutions that are classed as a medium-size or large enterprise in accordance with the ZGD-1.

6.1.1.2. Customer risk assessment

CRA risk criteria

The set of risk criteria that the payment institution must take into account as the minimum standard is cited below, although the obliged entity may also take account of additional criteria (defined in the guidelines or derived from the obliged entity's business) or treat the below criteria more strictly.

CUSTOMER LEGAL/NATURAL PERSON	CUSTOMER RISK CRITERIA	RISK LEVEL
NP/LP	The customer is a resident	LR

LP	An undertaking listed on a securities market to which disclosure requirements and requirements for adequate transparency of the BO apply	LR
LP	An undertaking under 100% ownership of the Republic of Slovenia	LR
LP	Undertakings that disclose ownership on the basis of bearer shares, where the ownership is evident from the record of holders of bearer shares at KDD	MR
NP/LP	The customer is a non-resident	MR
NP/LP	Other customers that are not classed as high-risk or low-risk	MR
NP	The customer's identity was verified on the basis of a temporary residence permit or an asylum-seeker's ID card	IR
NP/LP	Indicators of suspected ML/TF have been flagged in connection with the customer or a related party, for example: ▪ there is no economic logic to the business in Slovenia (e.g. the customer has a registered office and executes transactions outside the geographical region of the payment institution and the purpose of transactions of this type is not evident); ▪ the customer appears to be acting on behalf of another person (e.g. a third party controls/oversees the customer, the customer reads written instructions); ▪ the customer's transactions are always just below the thresholds for reporting, etc.; ▪ the customer uses services in an unusual way (e.g. sends money to himself/herself/itself or receives it from himself/herself/itself, or sends it immediately after receiving it); ▪ the customer knows very little about the payee, or does not want to provide information about the payee; ▪ multiple corporate customers transfer funds to the same payee, or the payee identity information, e.g. the address or telephone number, appears to be the same; ▪ the required information about the payer or the payee has not been provided for an executed transaction; ▪ the amount sent or received does not accord with the customer's revenues (if known).	IR
NP/LP	An enquiry has been received from the FIU for the customer, its statutory representative, its authorised representative or the BO	IR
LP	The undertaking's ownership structure is unusual or overly complicated relative to the nature of its business	IR
LP	Customers whose business activity is highly cash-intensive	IR
NP/LP	The customer or the BO is a PEP, a close family member of a PEP, or a close associate of a PEP	HR
NP/LP	The customer, its statutory representative, its authorised representative or the BO has been reported to the FIU for suspected ML/TF	HR
NP/LP	The FIU has submitted a transaction monitoring request or an asset freeze request for the customer	HR
NP/LP	The customer, its statutory representative, its authorised representative or the BO is on a list of persons, groups and entities involved in terrorist acts to whom EU restrictive measures apply (e.g. FBE)	HR
LP	Undertakings that disclose ownership on the basis of bearer shares, where the customer discloses ownership on the basis of a contract, notarial protocol or share register of a foreign authority	HR

CUSTOMER LEGAL/NATURAL PERSON	**COUNTRY RISK CRITERIA**	**RISK LEVEL**
NP/LP	The customer, statutory representative, authorised representative or BO has a registered office, domicile or temporary residence or is a citizen of an EU Member State or the EEA	LR
NP/LP	The customer, statutory representative or authorised representative has a registered office, domicile or temporary residence or is a citizen of a third country	MR
NP/LP	The customer, statutory representative or authorised representative has a registered office, domicile or temporary residence or is a citizen of a country that is on the list of high-risk third countries or on the list of increased-risk countries	HR

It is recommended for payment institutions to draw up their own list of geographical regions, and in doing so may assess individual geographical regions differently from the approach proposed in the above table. Notwithstanding the above, obliged entities must always assess and treat geographical regions on the list of high-risk third countries as high-risk geographical regions.

CUSTOMER LEGAL/NATURAL PERSON	PRODUCT/SERVICE/TRANSACTION RISK CRITERIA	RISK LEVEL
NP/LP	The settlement of liabilities for executed payments and cash withdrawals is executed via current accounts of customers or a UPO at a bank inside the EEA	LR
NP/LP	Products and services that pose an increased risk: • products that allow for transactions of large or unlimited value; • products and services that are reachable worldwide.	IR
NP/LP	Other products/services that the obliged entity assesses as an increased risk	IR
NP/LP	Transactions that pose increased risk and are taken into account within the framework of transaction monitoring, and could have an impact on the CRA: • transactions executed in cash; • transactions executed by payers from different countries to the account of the same payee; • transactions related to countries on the list of high-risk third countries; • other transactions that the obliged entity assesses as an increased risk.	IR

CUSTOMER LEGAL/NATURAL PERSON	DISTRIBUTION CHANNEL RISK CRITERIA	RISK LEVEL
NP/LP	The business relationship is entered into in the personal presence of the customer or the statutory representative	LR
NP/LP	The business relationship is entered into by means of electronic identification with a high degree of reliability	LR
NP/LP	The business relationship is entered into by means of video-based electronic identification	MR
NP/LP	The business relationship is entered into by other means of establishing and verifying identity	MR
NP/LP	The business relationship is entered into via an authorised representative	MR
NP/LP	The business relationship is entered into via an external service provider	MR
NP/LP	The business relationship is entered into via a third party	MR

Definition of initial CRA and updating of CRA

Payment institutions are required to manage the information on customer risk category within the framework of their IT support. This is not required for payment institutions that are classed as a micro or small enterprise in accordance with the ZGD-1. If the payment institution does not manage information within its IT support, it should be kept in the documentation obtained as part of concluding a business relationship and during review and updating of information and documentation.

The recommendation from the general guidelines for putting in place IT support that enables automatic execution of the CRA and a definition of the customer risk category, does not apply to payment institutions that due to their limited offer of products and services associated with providing payment services and/or a low number of users of such services, can effectively conduct the CRA without the use of IT support.

6.1.2. Customer due diligence

6.1.2.1. Scope of due diligence with regard to CRA

Review of political exposure

The requirement under the general guidelines to put in place a procedure for automatically determining the political exposure of customers and BOs using commercial PEP databases (e.g. Dow Jones WatchList, World Check) applies only to payment institutions that are classed as a medium-size or large enterprise in accordance with the ZGD-1. The procedure of automatic determining of PEP is a recommendation for other payment institutions. A payment institution that does not put in place automatic reviewing should determine the political exposure of the customer or BO by obtaining a statement of the customer, statutory representative or authorised representative and based on information learned from other sources (*e.g. customer performs function deemed to be a prominent public position*[17]).

6.1.3. Transaction monitoring

Transaction monitoring

To ensure effective risk management in the area of AML/CFT, payment institutions are recommended to put in place adequate IT support for transaction monitoring. A payment institution that does not put in place IT support must provide for a system based on which it will conduct effective monitoring of customer transactions.

Review and updating of information and documentation

The recommendation under the general guidelines to put in place IT support that will warn employees of the need to review and update the information and documentation about the customer and will also include an audit trail with regard to the due diligence conducted, only applies to payment institutions payment institutions that are classed as a medium-size or large enterprise in accordance with the ZGD-1. Other payment institutions must have in place a system that will ensure that the review and updating of documentation and information on the customer are conducted in a timely manner and properly recorded.

6.1.4. Customer acceptance policy

Payment institutions must adopt a customer acceptance policy through which they define their intentions with regard to doing business with customers covered by individual CRAs. Payment institutions should embed this policy in its existing internal policies or adopt a stand-alone bylaw.

[17] Details available in the currently valid Decree on the exact functions which qualify as prominent public functions in the Republic of Slovenia.

6.2. Sectoral guidelines for e-money issuers

These sectoral guidelines apply to obliged entities that are e-money issuers. E-money issuers should also take account of the ML/TF risk factors guidelines, especially Guideline 10: Sectoral guideline for electronic money issuers and Guideline 11: Sectoral guideline for money remitters.

ML/TF risks in transactions in electronic money relate primarily to the risks inherent in the actual service of issuing electronic money and the related products, and in the customers who use such products and services.

6.2.1. Risk assessment

In accordance with Article 18 of the ZPPDFT-2 and the guidelines, e-money issuers draw up an OERA and CRA and implement AML/CFT measures depending on the risk identified.

E-money issuers should update the **OERA** and review and update the risk criteria and **CRA** methodology **at least once every two (2) years**.

6.2.1.1. Obliged entity's risk assessment

OERA methodology

1. *Inherent risk*

In assessing inherent risk, e-money issuers should take into account the following product risk criteria:

- electronic money (*e.g. volume of electronic money of residents/non-residents*);
- electronic wallet (*e.g. volume of cash top-ups using UPN forms, current account or other electronic wallet*);
- cards or similar devices (*e.g. scope of use in/outside Slovenia);*
- other products provided by e-money issuers.

2. *Control environment*

E-money issuers assess the control environment within the framework of the areas set out in the general guidelines, except for:

- relative to the size and the organisation, e-money issuers that are classed as a micro or small enterprise in accordance with the ZGD-1 are not required to assess the areas of **Reporting** and **Independent audit**;
- in cases where the AML/CFT officer and/or their deputies do not perform this function exclusively, in the area of **AML/CFT function** an assessment is made as to whether they are allowed to effectively perform the duties of the AML/CFT officer and the deputy in accordance with Article 85 of the ZPPDFT-2.

Obliged entity's measures on the basis of the OERA

The requirement under the general guidelines that the responsible employees at the obliged entity (the AML/CFT officer, the responsible management board members, or other employees) present the results of the OERA to the persons responsible for individual business lines and to the internal audit department (point 3 of the first paragraph of Section 2.2.2 Obliged entity's measures on the basis of the OERA) is not binding on e-money issuers. Notwithstanding the above, this measure is recommended for e-money issuers that are classed as a medium-size or large enterprise in accordance with the ZGD-1.

6.2.1.2. Customer risk assessment

CRA risk criteria

The set of risk criteria that e-money issuers must take into account as the minimum standard is cited below, although the obliged entity may also take account of additional criteria (defined in

the guidelines or derived from the obliged entity's business) or treat the below criteria more strictly.

CUSTOMER LEGAL/NATURAL PERSON	CUSTOMER RISK CRITERIA	RISK LEVEL
NP/LP	The customer is a resident	LR
NP/LP	The customer is a non-resident	MR
NP	The customer's identity was verified on the basis of a temporary residence permit or an asylum-seeker's ID card	IR
NP/LP	An enquiry has been received from the FIU for the customer, its statutory representative, its authorised representative or the BO	IR
NP/LP	Indicators of suspected ML/TF have been identified in connection with the customer or a related party, for example: ▪ the customer or a related party is behaving unusually or suspiciously; ▪ the customer has failed to provide adequate clarifications with regard to the economic logic of the intended transactions; ▪ there is doubt as to the credibility or relevance of the submitted documentation; ▪ the customer requests secrecy when entering into the business relationship, and does not wish to disclose the requisite information during due diligence.	IR
NP/LP	The customer or the BO is a PEP, a close family member of a PEP, or a close associate of a PEP	HR
NP/LP	The customer, its statutory representative, its authorised representative or the BO has been reported to the FIU for suspected ML/TF	HR
NP/LP	The FIU has submitted a transaction monitoring request or an asset freeze request for the customer	HR
NP/LP	The customer, its statutory representative, its authorised representative or the BO is on a list of persons, groups and entities involved in terrorist acts to whom EU restrictive measures apply (e.g. FBE)	HR

CUSTOMER LEGAL/NATURAL PERSON	COUNTRY RISK CRITERIA	RISK LEVEL
NP/LP	The customer, statutory representative, authorised representative or BO has a registered office, domicile or temporary residence or is a citizen of an EU Member State or the EEA	LR
NP/LP	The customer, statutory representative, authorised representative or BO has a registered office, domicile or temporary residence or is a citizen of a third country	MR
NP/LP	The customer, statutory representative, authorised representative or BO has a registered office, domicile or temporary residence or is a citizen of a country that is on the list of high-risk third countries or on the list of increased-risk countries	HR

It is recommended for e-money issuers to draw up their own list of geographical regions, and in doing so may assess individual geographical regions differently from the approach proposed in the above table. Notwithstanding the above, e-money issuers must always assess and treat geographical regions on the list of high-risk third countries as high-risk geographical regions.

CUSTOMER LEGAL/NATURAL PERSON	PRODUCT/TRANSACTION RISK CRITERIA	RISK LEVEL
NP/LP	Payment instruments for which the obliged entity has obtained consent from the FIU in accordance with the ZPPDFT-2 to omit certain customer due diligence measures in connection with electronic money	LR
NP/LP	Other products that the obliged entity assesses as a low risk	LR
NP/LP	Payment instruments that pose an increased risk: • have no (monthly) limits or allow very high limits; • do not have restrictions with regard to an individual payment;	IR

	• allow for cash withdrawals; • can be used for other purposes (and not solely for the purchase of goods and services); • can be loaded with anonymous electronic money; • allow inward payments by third parties whose identity is not disclosed; • can be used in a large number of points of sale (multiple merchants).	
NP/LP	Transfers of funds that pose increased risk and are taken into account within the framework of transaction monitoring, and could have an impact on the CRA: • the customer purchases several payment instruments from the same issuer, frequently reloads the payment instrument or executes multiple cash withdrawals over a short period and without any economic logic; • the customer's fund transfers are always just below the threshold; • the payment instrument appears to be used by several people whose identity is not known to the issuer (e.g. the product is used from multiple IP addresses at the same time); • the customer's identification data changes frequently (e.g. home address, IP address or linked bank accounts); • the payment instrument is not used in accordance with the stated purpose (e.g. it is used in the rest of the world, even though it is designed as a gift card for a shopping centre); • other transfers of funds that the obliged entity assesses as an increased risk.	IR

CUSTOMER LEGAL/NATURAL PERSON	DISTRIBUTION CHANNEL RISK CRITERIA	RISK LEVEL
NP/LP	The business relationship is entered into in the personal presence of the customer or the statutory representative	LR
NP/LP	The business relationship is entered into by means of electronic identification with a high degree of reliability	LR
NP/LP	The business relationship is entered into by means of video-based electronic identification	MR
NP/LP	The business relationship is entered into by other means of establishing and verifying identity	MR
NP/LP	The business relationship is entered into via an authorised representative	MR
NP/LP	The business relationship is entered into via an external service provider	MR
NP/LP	The business relationship is entered into via a third party	MR

Definition of initial CRA and updating of CRA

E-money issuers are required to manage the information on customer risk category within the framework of their IT support. This is not required for e-money issuers that are classed as a micro or small enterprise in accordance with the ZGD-1 and for which the IT-supported management of information on customer risk category is recommended. If the e-money issuer does not manage information within its IT support, it should be kept in the documentation obtained as part of entering into a business relationship and during the review and updating of information and documentation.

The recommendation from the general guidelines for putting in place IT support that enables automatic execution of the CRA and a definition of the customer risk category, does not apply to e-money issuers that due to their limited offer of products associated with the issuance of e-money and/or a low number of users of such products can effectively conduct the CRA without the use of IT support.

6.2.1. Customer due diligence

6.2.1.1. Scope of due diligence with regard to CRA

Review of political exposure

The requirement under the general guidelines to put in place up a procedure for automatically determining the political exposure of customers and BOs using commercial PEP databases (e.g. Dow Jones WatchList, World Check) applies only to e-money issuers that are classed as a medium-size or large enterprise in accordance with the ZGD-1. The procedure of automatic determining of PEP is a recommendation for other e-money issuers. An e-money issuer that does not put in place automatic reviewing should determine the political exposure of the customer or BO by obtaining a statement of the customer, statutory representative or authorised representative and based on information learned from other sources (*e.g. customer performs function deemed to be a prominent public position*[18]).

6.2.1. Transaction monitoring

Transaction monitoring

To ensure effective risk management in the area of AML/CFT, e-money issuers are recommended to put in place adequate IT support for transaction monitoring. An e-money issuer that does not put in place IT support must provide for a system based on which it will conduct effective monitoring of customer transactions.

Review and updating of information and documentation

E-money issuers must put in place a system to ensure that the review and updating of documentation and information on the customer are conducted in a timely manner and properly recorded.

6.2.2. Customer acceptance policy

E-money issuers are recommended to adopt a customer acceptance policy through which they define their intentions with regard to doing business with customers covered by individual CRAs. If an e-money issuer adopts the aforementioned policy, it should embed this policy in its existing internal policies or adopt a stand-alone bylaw.

[18] Details available in the currently valid Decree on the exact functions which qualify as prominent public functions in the Republic of Slovenia.

6.3. Sectoral guidelines for currency exchange offices

This section applies to obliged entities that are currency exchange offices. Currency exchange offices should also take account of the ML/TF risk factors guidelines, especially Guideline 19: Sectoral guidelines for firms providing activities of currency exchange offices.

The key risk criteria that raise ML/TF risks at currency exchange offices include the often cash-based character of the transactions, the anonymity of transactions, operations in border areas, and business in occasional transactions, conducted for the most part by customers in transit (tourists, cross-border workers, migrants and asylum-seekers). Currency exchange offices are thus required to assess the risks inherent in their business with occasional customers, and to put in place appropriate policies, controls and procedures for the purposes of managing the identified ML/TF risks.

Under the principle of proportionality, currency exchange offices should also take into account the simplicity of their transactions and the size (especially sole traders and micro enterprises), or perform currency exchange services as an exclusive or main activity or as an additional or side activity (e.g. as part of operating a hotel, shop, catering establishment, hairdressing) and the fact that currency exchange services score a low national ML/TF risk assessment.

6.3.1. Risk assessment

In accordance with Article 18 of the ZPPDFT-2 and the guidelines, currency exchange offices draw up an OERA and implement AML/CFT measures depending on the risk identified. Applying the principle of proportionality, a comprehensive and complex OERA is not envisaged for currency exchange offices (*details in Section 6.3.2 Obliged entity's risk assessment*). The **OERA** should be updated **every two (2) years**.

The requirements under the general guidelines with regard to the **CRA** (*Section 2.3. Customer risk assessment*) are not fully binding on currency exchange offices; instead they apply *mutatis mutandis* only with regard to the **risk criteria for determining the scope of customer due diligence in the execution of occasional transactions** (*for details see Section 6.3.3 Sectoral guidelines in risk assessment and customer due diligence*).

6.3.1.1. Obliged entity's risk assessment

Methodology

In preparing the OERA, currency exchange offices should take into account the following criteria for assessing inherent risk and the areas based on which obliged entities assess the control environment.

CURRENCY EXCHANGE OFFICE'S RISK ASSESSMENT		
Inherent risk	**Control environment**	**Residual risk**
• Customers (PEP, resident, non-resident) • Transactions • Other risks	• Policies and procedures • Customer due diligence during execution of occasional transactions • Record-keeping and data storage • AML/CFT officer • Identification and reporting of suspected ML/TF • Training • Supervisory measures	On the basis of the assessments of inherent risk and the control environment, residual risk is assessed as follows: • **low risk** • **medium risk** • **high risk**

In its OERA analysis the currency exchange office should also take account of those risk criteria and control environment areas which can be assessed as impacting its ML/TF risk.

Obliged entity's measures on the basis of the OERA
The requirement under the general guidelines that the responsible employees at the obliged entity (the AML/CFT officer, the responsible management board members, or other employees) present the results of the OERA to the persons responsible for individual business lines and to the internal audit department (point 3 of the first paragraph of Section 2.2.2 Obliged entity's measures on the basis of the OERA), is not binding on currency exchange offices. Notwithstanding the above, this measure is recommended for currency exchange offices that are classed as a medium-size or large enterprise in accordance with the ZGD-1.

6.3.1.2. Risk assessment during execution of occasional transactions
Under the ZPPDFT-2, when executing currency exchange operations in excess of EUR 1,000 the obliged entity is required to conduct customer due diligence, and to:
- establish the identity of the customer, its statutory representative or authorised representative and to verify the customer's identity on the basis of credible, independent and objective resources;
- identify the customer's BO;
- obtain information about the purpose of the transaction.

CRA criteria
In executing occasional transactions, currency exchange offices should assess the risk and determine the scope of customer due diligence, and consequently the necessary AML/CFT measures. The **risk criteria affecting the scope of customer due diligence** with regard to the execution of currency exchange operations are:

CUSTOMER LEGAL/NATURAL PERSON	CUSTOMER RISK CRITERIA	RISK LEVEL
NP/LP	The customer is a resident	LR
NP/LP	The customer is a non-resident	MR
LP	Undertakings that disclose ownership on the basis of bearer shares, where the ownership is evident from the record of holders of bearer shares at KDD	MR
NP	The customer's identity was verified on the basis of a temporary residence permit or an asylum-seeker's ID card	IR
NP/LP	Indicators of suspected ML/TF have been identified in connection with the customer or a related party, for example: ▪ the customer or a related party is behaving unusually or suspiciously; ▪ the customer avoids providing the required information; ▪ there is doubt as to the credibility or relevance of the submitted documentation; ▪ the customer appears to be acting on behalf of another person (e.g. a third party controls/oversees the customer, the customer reads written instructions).	IR
NP/LP	An enquiry has been received from the FIU for the customer, its statutory representative, its authorised representative or the BO	IR
NP/LP	The undertaking's ownership structure is unusual or overly complicated relative to the nature of its business	IR
	Undertakings operating in the following industries or whose business activities are as follows: • money services (money services business); • issuance, brokerage and storage of virtual assets, and other activities related to virtual assets; • non-governmental and non-profit organisations; • charitable organisations;	IR

	• manufacturers and traders of armaments and other military equipment; • mining and quarrying; • petroleum and natural gas; • construction; • pharmaceuticals; • sale and brokerage of real estate; • sale of gold and other precious metals; • sale and brokerage of valuable goods and high-value assets (e.g. yachts, cars, works of art and antiques); • casinos and other games of chance (betting shops, online games of chance, etc.).	
NP/LP	The customer or the BO is a PEP, a close family member of a PEP, or a close associate of a PEP	HR
NP/LP	The customer, its statutory representative, its authorised representative or the BO has been reported to the FIU for suspected ML/TF	HR
NP/LP	The FIU has submitted a transaction monitoring request or an asset freeze request for the customer	HR
NP/LP	Undertakings that disclose ownership on the basis of bearer shares, where the customer discloses ownership on the basis of a contract, notarial protocol or share register of a foreign authority	HR
NP/LP	The customer, its statutory representative, its authorised representative or the BO is on a list of persons, groups and entities involved in terrorist acts to whom EU restrictive measures apply (e.g. FBE)	HR

CUSTOMER LEGAL/NATURAL PERSON	**COUNTRY RISK CRITERIA**	**RISK LEVEL**
NP/LP	The customer, statutory representative, authorised representative or BO has a registered office, domicile or temporary residence in an EU Member State or the EEA	LR
NP/LP	The customer, statutory representative, authorised representative or BO has a registered office, domicile or temporary residence in a third country	MR
NP/LP	The customer, statutory representative, authorised representative or BO has a registered office, domicile or temporary residence in a country that is on the list of high-risk third countries or on the list of increased-risk countries	HR

Currency exchange offices may draw up their own list of geographical regions, and may assess individual geographical regions differently from the approach proposed in the above table. Notwithstanding the above, currency exchange offices must always assess and treat geographical regions on the list of high-risk third countries as high-risk geographical regions.

CUSTOMER LEGAL/NATURAL PERSON	**TRANSACTION RISK CRITERIA**	**RISK LEVEL**
NP/LP	Transactions that pose an increased risk and are taken into account during the execution of currency exchange operations and within the framework of transaction monitoring: • currency exchange is executed by the customer, although this is not usually its registered business activity; • the source of funds is not known and the customer does not wish to disclose it; • smurfing; • the customer's transactions are just below the thresholds for reporting to the FIU; • currency exchange into a particular currency, and immediate exchange into another currency; • other unusual circumstances in the execution of transactions (e.g. significant and unexplained geographical distance between the currency exchange office and the customer's domicile); • currency exchange into the currencies of countries on the list of high-risk third countries;	IR

	• other transactions that the obliged entity assesses as an increased risk.	

Currency exchange offices are not governed by the requirements of the general guidelines regarding the preparation of the CRA methodology (Section 2.3.2 CRA methodology), but they should draw up a **methodology** for the scope of customer due diligence during the execution of currency exchange operations as follows:

RISK CRITERIA LEVEL	SCOPE OF DUE DILIGENCE
LR	Simplified
MR	Standard
IR	Standard/enhanced
HR	Enhanced

One or more risk criteria related to the customer or the currency exchange operation may influence the scope of customer due diligence.

In the case of multiple criteria, the risk criterion **whose risk level is highest** is taken into account (*e.g. the currency exchange is executed by a resident who is a PEP: because PEP status is a high-risk criterion, the obliged entity conducts enhanced due diligence*).

Currency exchange offices should define the criteria and methodology for the scope of customer due diligence in internal policies and should review them and **as necessary update them at least once every two (2) years**.

Due to the nature of their operations, currency exchange offices are not required to implement measures to define an initial CRA and or to update the CRA (Section 2.3.3).

6.3.2. Customer due diligence

6.3.2.1. Establishment and verification of customer's identity

When executing occasional transactions, currency exchange offices should conduct in-person customer due diligence of the customer, the statutory representative or the authorised representative (*for details see Section 3.1.1 Customer due diligence in person*).

6.3.2.2. Scope of due diligence during execution of occasional transactions

Currency exchange offices obtain information relevant for determining the risk criteria prior to executing occasional transactions, and in view of the identified risk they conduct simplified, standard or enhanced customer due diligence. The obliged entity takes account of the guidelines when carrying out measures with regard to the scope of due diligence (*for details see Section 3.2 Scope of due diligence with regard to CRA*).

Currency exchange offices **record the scope of the due diligence** conducted prior to the occasional transaction, and **store the information and documentation obtained** in accordance with the requirements of the ZPPDFT-2.

Review of political exposure

The requirement under the general guidelines to put in place a procedure for automatically determining the political exposure of customers and BOs using commercial PEP databases (e.g. Dow Jones WatchList, World Check) is not binding on currency exchange offices. This measure is recommended for currency exchange offices that are classed as a medium-size or large enterprise in accordance with the ZGD-1. A currency exchange office that does not put in place automatic reviewing should determine the political exposure of the customer or BO by obtaining a statement of the customer, statutory representative or authorised representative and based on

information learned from other sources (*e.g. customer performs function deemed to be a prominent public position*[19]).

6.3.3. Transaction monitoring

Due to the nature of their operations, currency exchange offices are not required to implement transaction monitoring measures.

6.3.4. Customer acceptance policy

The requirements of the guidelines with regard to the customer acceptance policy (*Section 5.1. Customer acceptance policy*) are not binding on currency exchange offices.

6.4. Sectoral guidelines for virtual currency service providers

This section applies to obliged entities that are virtual currency service providers. In line with the supranational risk assessment and the national risk assessment, due to their design and the characteristics stemming from them, virtual currency services are more prone to ML/TF risk. The ZPPDFT-2 (point 19č of the first paragraph of Article 4 in connection with point 48 of Article 3) expanded the set of virtual currency service providers that must abide by the provisions of the aforementioned law and by AML/CFT measures in providing their products and services.

It is recommended that virtual currency service providers also take into account the international FATF standards, including:

- Guidance for a Risk-based approach – Virtual Assets and Virtual Asset Service Providers (June 2019);
- Virtual Assets – Red Flag Indicators of Money Laundering and Terrorist Financing (September 2020);
- Second 12 Month Review of the revised FATF Standards on Virtual Assets and Virtual Assets Service Providers (July 2021);
- Virtual Currencies – Key Definitions and Potential AML/CFT Risks (FATF, June 2014).

6.4.1. Risk assessment

In accordance with Article 18 of the ZPPDFT-2 and the guidelines, virtual currency service providers draw up an OERA and CRA and implement AML/CFT measures depending on the risk identified. Virtual currency service providers update their risk assessments in accordance with *Section 2.1.2 Updating of risk assessment*.

6.4.1.1. Obliged entity's risk assessment

OERA methodology

1. <u>Inherent risk</u>

In assessing inherent risk, virtual currency service providers should take into account the following product/service/transaction risk criteria:

a) services:
   - exchange between fiat and virtual currencies (*e.g. volume of exchange relative to the type of virtual currency (such as BTC, ETH, USDT, XMR); volume of exchange via ATM/web platform/in person*);

[19] Details available in the currently valid Decree on the exact functions which qualify as prominent public functions in the Republic of Slovenia.

- exchange between one or more types of virtual currencies (*e.g. volume of exchange relative to the type of virtual currency (such as BTC, ETH, USDT, XMR); volume of exchange via ATM/web platform/in person*); transfer of virtual currencies between various accounts or addresses (*e.g. volume of transfers, number of accounts or addresses*);
- storage of virtual currencies (*e.g. assets on cut-off date, number of customers*);
- managing virtual currencies (*e.g. assets under management with regard to the type of virtual currency*);
- providing services of protecting private cryptography keys (*e.g. number of users*);
- in connection with the issue and sale of virtual currencies (*e.g. volume of issued virtual currencies relative to the volume of sold currencies, having regard for customer risk*);
- other services offered by virtual currency service providers in connection with virtual currency services;

b) transactions: volume of transactions in view of country risk (*e.g. volume of assets in fiat currencies and virtual currencies from or into countries that are on the list of high-risk third countries; volume of cash transactions for exchange purposes*).

If virtual currency service providers organise their operations across individual lines, it is recommended that their inherent risk be determined by lines (*e.g. transactions with customers that are natural persons and transactions with customers that are legal persons; transactions with other virtual currency service providers, such as currency exchange offices*) or by products (*e.g. ATMs, custodian wallet providers, currency exchange offices*).

Obliged entity's measures on the basis of the OERA

The requirement under the general guidelines that the responsible employees at the obliged entity (the AML/CFT officer, the responsible management board members, or other employees) present the results of the OERA to the persons responsible for individual business lines and to the internal audit department (point 3 of the first paragraph of Section 2.2.2 Obliged entity's measures on the basis of the OERA) is not binding on virtual currency service providers. Notwithstanding the above, this measure is recommended for virtual currency service providers that are classed as a medium-size or large enterprise in accordance with the ZGD-1.

6.4.1.2. Customer risk assessment

CRA risk criteria

Below is a selection of risk criteria that virtual currency service providers must meet in order to make a customer risk assessment, in the scope that is relevant for them given their operations or business model. Virtual currency service providers may also take account of additional criteria (defined in the general guidelines or derived from the provider's business) or treat the below criteria more strictly.

CUSTOMER LEGAL/NATURAL PERSON	CUSTOMER RISK CRITERIA	RISK LEVEL
NP/LP	The customer is a resident	LR
LP	An undertaking listed on a securities market to which disclosure requirements and requirements for adequate transparency of the BO apply	LR
LP	A credit or financial institution established in an EU Member State or a third country that has put in place adequate AML/CFT mechanisms	LR
NP/LP	The customer is a non-resident	MR
LP	Undertakings that disclose ownership on the basis of bearer shares, where the ownership is evident from the record of holders of bearer shares at KDD	MR
NP	The customer's identity was verified on the basis of a temporary residence permit or an asylum-seeker's ID card	IR

NP/LP	Negative information has been obtained in connection with the customer, its statutory representative, its authorised representative or the BO	IR
NP/LP	An enquiry has been received from the FIU for the customer, its statutory representative, its authorised representative or the BO	IR
NP/LP	Indicators of suspected ML/TF have been identified in connection with the customer or a related party, for example: ▪ the customer or a related party is behaving unusually or suspiciously; ▪ the customer appears to be acting on behalf of another person (e.g. a third party controls/oversees the customer, the customer reads written instructions) and does not provide information on who the other person is; ▪ the customer declines the request to submit documents as part of customer due diligence; ▪ there is doubt as to the credibility or relevance of the submitted documentation; ▪ the customer suddenly breaks off the business relationship, especially if they pay unusually high fees for breaking it off; ▪ the customer frequently changes identification information, including their e-mail, IP-address or financial data.	IR
NP/LP	The customer's virtual currency address appears on public forums associated with illegal activity	IR
LP	Undertakings operating in industries or whose business activities are as follows:[20] • money services (money services business); • virtual currency services or other transactions included in such services; • non-governmental and non-profit organisations; • charitable organisations; • manufacturers and traders of armaments and other military equipment; • mining and quarrying; • petroleum and natural gas; • construction; • pharmaceuticals; • sale and brokerage of real estate; • sale of gold and other precious metals; • sale and brokerage of valuable goods and high-value assets (e.g. yachts, cars, works of art and antiques); • online casinos and other online games of chance (betting shops, online games of chance, etc.).	IR
LP	The undertaking's ownership structure is unusual or overly complicated relative to the nature of its business	IR
LP	Sudden changes in the ownership structure or ultimate BO that cannot be explained	IR
LP	The customer is a legal person or another entity of foreign law established for a specific purpose (a special-purpose vehicle [SPV] or trust)	IR
LP	There is credible information about a customer that is a virtual currency service provider or is a financial institution that supervisory measures for the rectification of irregularities in the area of AML/CFT or administrative fines have been imposed on it by supervisory authorities	IR
LP	The customer operates as an unregistered/unlicensed virtual currency service provider[21] or on P2P online exchange sites	IR

[20] When identifying a legal person's higher-risk business activities, obliged entities may make use of various resources (e.g. the standard classification of activities [SKD] or the European classification of economic activities [NACE] that are classed as higher-risk activities and industries; CNVOS's list of NGOs; the register of humanitarian organisations; the register of providers engaged in exchange services between virtual currencies and fiat currencies and custodian wallet providers administered by the FIU). In the CRA the obliged entity also takes account of information about an undertaking's industry or business activities that pose an increased risk, if the information is obtained from the customer or is identified (or should be identified with regard to the available information) as part of transaction monitoring.

[21] The virtual currency service provider checks whether the customer is registered or licensed for the purposes of AML/CFT (e.g. in Slovenia the virtual currency service providers that have a registered office or branch in Slovenia must

NP/LP	The customer or the BO is a PEP, a close family member of a PEP, or a close associate of a PEP	HR
NP/LP	The customer, its statutory representative, its authorised representative or the BO has been reported to the FIU for suspected ML/TF	HR
NP/LP	The FIU has submitted a transaction monitoring request or an asset freeze request for the customer	HR
NP/LP	The customer uses an IP address associated with the darknet, or other similar software that enables anonymous communication	HR
NP/LP	The customer, its statutory representative, its authorised representative or the BO is on a list of persons, groups and entities involved in terrorist acts to whom EU restrictive measures apply (e.g. FBE)	HR
LP	Undertakings that disclose ownership on the basis of bearer shares, where the customer discloses ownership on the basis of a contract, notarial protocol or share register of a foreign authority	HR

Virtual currency service providers that only provide their services in the territory of the Republic of Slovenia should apply **the following country risk criteria**:

CUSTOMER LEGAL/NATURAL PERSON	**COUNTRY RISK CRITERIA**	**RISK LEVEL**
NP/LP	The customer, statutory representative, authorised representative or BO has a registered office, domicile or temporary residence or is a citizen of an EU Member State or the EEA	LR
NP/LP	The customer, statutory representative, authorised representative or BO has a registered office, domicile or temporary residence or is a citizen of a third country	MR
NP/LP	The customer, statutory representative, authorised representative or BO has a registered office, domicile or temporary residence or is a citizen of a country that is on the list of high-risk third countries or on the list of increased-risk countries	HR

It is recommended for the above-stated providers to draw up their own list of geographical regions, and in doing so may assess individual geographical regions differently from the approach proposed in the above table. Notwithstanding the above, virtual currency service providers must always assess and treat geographical regions on the list of high-risk third countries as high-risk geographical regions.

Virtual currency service providers that provide their services across borders should apply **the country risk criteria as set out in the general part of the guidelines** (*details in Section 2.3.1.2 Country risk criteria).*

CUSTOMER LEGAL/NATURAL PERSON	**SERVICE/TRANSACTION RISK CRITERIA**	**RISK LEVEL**
NP/LP	Services that pose medium risk • storage of virtual currencies (e.g. balance of assets on cut-off date, number of customers); • providing services of protecting private cryptography keys; • exchange between fiat and virtual currencies; • other services that the obliged entity has assessed as posing medium ML/TF risk.	MR
NP/LP	Services that pose increased risk: • exchange between one or more types of virtual currency; • management of virtual currencies; • the issuance and sale of virtual currencies;	IR

be entered in the register kept by the FIU prior to beginning the provision of virtual currency services, in accordance with the ZPPDFT-2).

	• other services that the obliged entity has assessed as posing increased ML/TF risk.	
NP/LP	Transactions that pose increased risk and are taken into account within the framework of transaction monitoring, and could have an impact on the CRA: • smurfing; • high volume of transactions in a previously dormant account (brief period such as 24 hours; in an even and regular pattern – risk of malware); • transactions where the source of funds is not known; • deposit of virtual currency followed by immediate withdrawal of virtual currency or exchange into several different virtual currencies; • transactions that do not have a clear economically or legally justified purpose; • the number of transactions deviates from the customer's usual volume of business; • virtual currency transactions deviate from the customer's usual volume of business and are not proportionate to its activity; • the transactions deviate from the stated purpose of business; • transactions with countries on the list of countries that pose increased ML/TF risks; • transactions related to countries on the list of high-risk third countries.	IR
NP/LP	Services that represent high risk: • exchange between fiat and virtual currencies through ATMs that do not ensure appropriate identification of the customer; • exchange between one or more types of virtual currency through ATMs that do not ensure appropriate identification of the customer; • other services that the obliged entity has assessed as posing high ML/TF risk.	HR
NP/LP	Transactions that pose a high risk and are taken into account within the framework of transaction monitoring, and could have an impact on the CRA: • transactions in virtual currencies where there is a suspicion that they have been stolen or obtained fraudulently; • transfers of virtual currencies associated with tumblers; • transactions with known wallet addresses and the market on the darknet.	HR

For product/service/transaction risk criteria, the virtual currency service provider cannot assess the risk as low.

CUSTOMER LEGAL/NATURAL PERSON	**DISTRIBUTION CHANNEL RISK CRITERIA**	**RISK LEVEL**
NP/LP	The business relationship is entered into in the personal presence of the customer or the statutory representative	LR
NP/LP	The business relationship is entered into by means of electronic identification with a high degree of reliability	LR
NP/LP	The business relationship is entered into by means of video-based electronic identification	MR
NP/LP	The business relationship is entered into by other means of establishing and verifying identity	MR
NP/LP	The business relationship is entered into via an authorised representative	MR
NP/LP	The business relationship is entered into via an external service provider	MR
NP/LP	The business relationship is entered into via a third party	MR

Definition of initial CRA and updating of CRA

Virtual currency service providers are required to manage the information on customer risk category within the framework of their IT support. This is not required for virtual currency service providers that are classed as a micro or small enterprise in accordance with the ZGD-1 and that provide their services only in the territory of the Republic of Slovenia. If the virtual currency

service provider does not manage information within its IT support, it should be kept in the documentation obtained as part of entering into a business relationship and during review and updating of information and documentation.

The recommendation from the general guidelines for putting in place IT support that enables automatic execution of the CRA and a definition of the customer risk category, does not apply to virtual currency service providers that due to their limited offer of virtual currency services and the low number of customers using such services can effectively conduct the CRA without the use of IT support, provided that the provider is classed as a micro or small enterprise in accordance with the ZGD-1 and provides its services only in the territory of the Republic of Slovenia.

6.4.2. Customer due diligence

6.4.2.1. Scope of due diligence

Review of political exposure

The requirement under the general guidelines to put in place a procedure for automatically determining the political exposure of customers and BOs using commercial PEP databases (e.g. Dow Jones WatchList, World Check) applies to all virtual currency service providers, with the exception of virtual currency service providers that are classed as a micro or small enterprise in accordance with the ZGD-1 and provide their services only in the territory of the Republic of Slovenia. In this case the provider should determine the political exposure of the customer or BO by obtaining a statement of the customer, statutory representative or authorised representative and based on information learned from other sources (*e.g. customer performs function deemed to be a prominent public position*[22]).

6.4.3. Transaction monitoring

To ensure effective risk management in the area of AML/CFT, virtual currency service providers **must** put in place adequate IT support for transaction monitoring.

6.4.4. Prohibited transactions

Prohibited transactions

It should be especially underlined that virtual currency service providers **may not open, issue or administer for customers anonymous accounts or any other products that could directly or indirectly conceal the customer's identity** (*details in 5.2 Prohibited transactions*).

[22] Details available in the currently valid Decree on the exact functions which qualify as prominent public functions in the Republic of Slovenia.

7. Final provisions

These guidelines shall enter into force fifteen days after their publication in the Official Gazette of the Republic of Slovenia.

On the day that these guidelines enter into force, the Guidelines on the assessment of ML/TF risk of 15 November 2019 shall cease to be in force.

Obliged entities are required to bring their policies, controls and procedures into line with the guidelines within six months of the publication of the guidelines on the Banka Slovenije website.

Legal persons and individuals independently pursuing registered business activities that become obliged entities (e.g. new payment institutions, new virtual currency service providers) must render their operations compliant with these guidelines within 12 months.