BANKA SLOVENIJE
EUROSYSTEM

BANK OF SLOVENIA
Slovenska 35
1505 Ljubljana
Slovenia
Tel.: +386 1 47 19 000
www.bsi.si

Bank of Slovenia
hereby issues

Guidelines

on the assessment of the money laundering and terrorist financing risk

This document is a translation from Slovene language. In case of doubt or discrepancy in the two versions, guidelines in the Slovene language shall prevail.

CONTENTS

ABBREVIATIONS

AML/CFT	Anti-money laundering and countering the financing of terrorism
AML/CFT officer	Officer for anti-money laundering and countering the financing of terrorism
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
BCBS	Basel Committee on Banking Supervision
BO	Beneficial owner
BoS	Bank of Slovenia
EEA	European Economic Area (EU Member States plus Norway, Iceland and Lichtenstein)
e-money	Electronic money (the same meaning as defined in the law governing payment services and systems)
FATF	Financial Action Task Force
Guidelines	Guidelines on the assessment of the risk of money laundering and terrorist financing approved by the Governing Board of the Bank of Slovenia on 5 November 2019
Guidelines on risk factors	Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced 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 (JC 2017 37), issued by the European supervisors (EBA, ESMA and EIOPA) on 4 January 2018
KDD	Central Securities Clearing Corporation
KYC	Know your customer
List of countries with increased risk of ML/TF	List of countries in connection with which there is a high or increased risk of money laundering or terrorist financing, published on the FIU website
List of high-risk third countries	List of high-risk countries adopted by the European Commission as a delegated act on the basis of Article 10 of Directive 2015/849/EU
ML	Money laundering
Moneyval	Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism, Council of Europe
FIU	Office of the Republic of Slovenia for Money Laundering Prevention, Cankarjeva 5, 1000 Ljubljana (Slovenia's Financial Intelligence unit - FIU)
PEP	Politically exposed person
STR	Suspicious transaction report
TF	Terrorist financing
ZBS-1	Bank of Slovenia Act (Official Gazette of the Republic of Slovenia, Nos. 72/06 [official consolidated version], 59/11 and 55/17), in its currently applicable wording
ZOUPAMO	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, No. 127/06)
ZPPDFT-1	Law governing the prevention of money laundering and terrorist financing, in its currently applicable wording

Pursuant to Article 31 of the ZBS-1 and Article 154 of the ZPPDFT-1, at its meeting of 5 November 2019 the Governing Board of the Bank of Slovenia adopted the following:

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

1. Purpose, scope of application and definition of terms

1.1. Purpose

For the effective management of ML/FT risks, obliged entities are required under the ZPPDFT-1 to identify and assess such risks, and adjust their control environment to be commensurate with the assessed ML/FT risks.

In accordance with Article 154 of the ZPPDFT-1, the Bank of Slovenia is issuing these **guidelines**, with regard to the implementation of individual requirements of the ZPPDFT-1 relating to:

- preparation of the ML/FT risk assessment;
- definition of simplified due diligence measures;
- definition of enhanced due diligence measures; and
- definition of the procedure for identifying politically exposed customers.

With these guidelines, the Bank of Slovenia also took account of the **guidelines on risk factors**, which were issued on the basis of the AMLD in January 2018 by the European supervisory authorities (EBA, ESMA, EIOPA). Guidelines on risk factors directly appliedfor obliged entities referred to in point 1.2 of the guidelines in accordance with the Regulation on the application of the Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced 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. 14/18). The guidelines on risk factors set out the criteria for the customer risk assessment, whereby the aforementioned criteria also apply *mutatis mutandis* to the obliged entity risk assessment.

For the effective management of ML/FT risks, obliged entities should draw up or update policies, procedures and controls in accordance with the guidelines. Obliged entities are required to update policies, procedures and internal controls by the deadline defined in the final provisions (*see Section 6. Final Provisions*).

1.2. Scope of application

The guidelines are addressed to the following obliged entities as defined by the ZPPDFT-1:

1. **banks, savings banks and branches of foreign banks;**
2. **payment institutions and payment institutions with a waiver;**
3. **electronic money institutions and electronic money institutions with a waiver;**
4. **currency exchange offices.**

The guidelines also apply *mutatis mutandis* to **other obliged entities** for which the Bank of Slovenia is defined as a competent supervisory authority in accordance with the first paragraph of Article 151 of the ZPPDFT-1.

The set of 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/FT 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 AMLD and the ZPPDFT-1. Within the framework of the guidelines, terms have the following meanings:

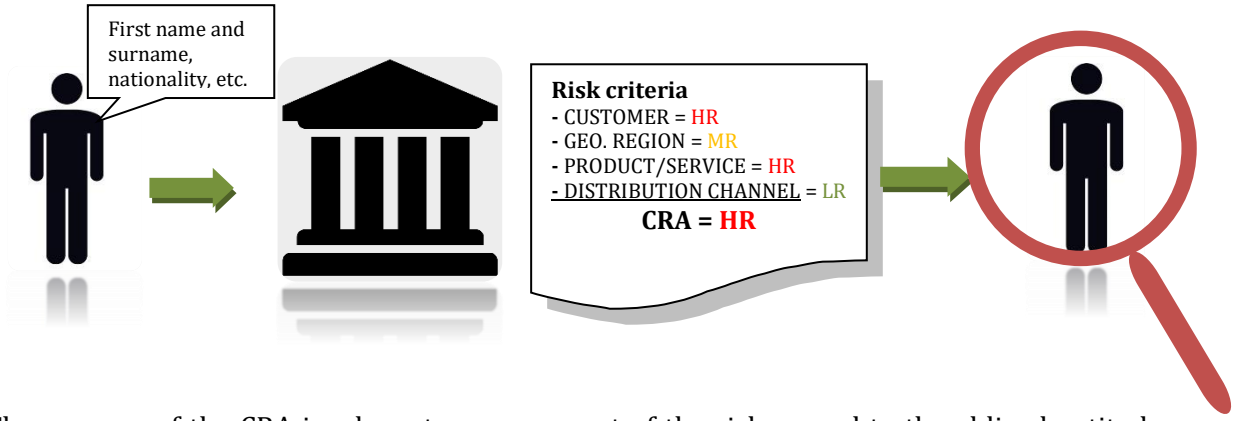
- an **obliged entity** is an entity that is an obliged entity in accordance with the first paragraph of Article 4 of the ZPPDFT-1, and for which the Bank of Slovenia is defined as a competent supervisory authority in accordance with the first paragraph of Article 151 of the ZPPDFT-1;
- a **supervisory authority** is a body responsible for conducting supervision of compliance with the requirements under the ZPPDFT-1, including compliance with the requirements relating to the assessment of ML/FT risks (Bank of Slovenia and the FIU);
- a **risk-based approach** is an approach in which the obliged entity identifies, assesses and understands the ML/FT 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/FT events occurring;
- **risk criteria** are variables that either alone or in combination with others could increase or reduce ML/FT 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/FT 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 **entity's risk assessment (ERA)** 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 business areas at the obliged entity that are exposed to ML/FT 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/FT purposes;
- the **customer risk category** denotes the level of ML/FT 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 ERA 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 business relationship with obliged entity;
- **resident/non-resident** have the same meaning as in the law governing foreign exchange operations.

2. About risk assessment

ML/FT risk is the risk that a customer will use the financial system for money laundering or terrorist financing, 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 money laundering or terrorist financing (first paragraph of Article 13 of the ZPPDFT-1).

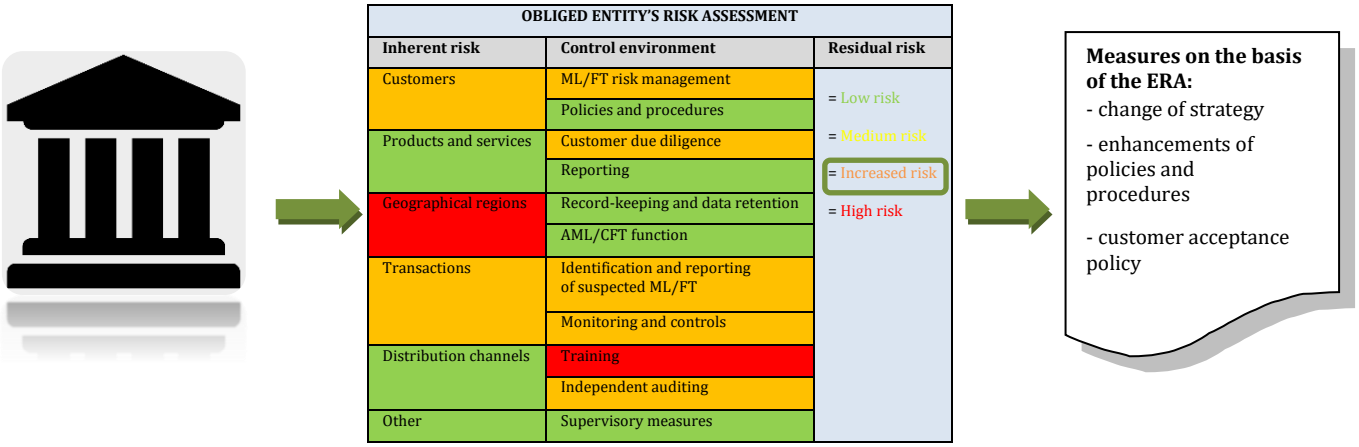
Under the ZPPDFT-1, an obliged entity is required to assess ML/FT risks in its operations, and on this basis is required to put in place policies, procedures and controls for the effective mitigation of ML/FT risks, and in so doing is required to perform one of the key AML/CFT tasks, which is carrying out customer due diligence measures.

By carrying out customer due diligence measures, obliged entities obtain information about the customer, and together 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 a ML/FT risk - the **customer risk assessment (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 customer's transaction monitoring, 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 referred to in point 1 of Section 1.2 of the guidelines (*see Section 1.2 Scope of application*) also draw up an **entity's risk assessment (ERA)**, 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 ERA, obliged entities referred to in point 1 of Section 1.2 of the guidelines identify ML/FT risks at the level of the obliged entity as a whole, which forms the basis for adopting appropriate measures to reduce the identified ML/FT risks.



2.1. Obliged entity's responsibility

Under the risk-based approach, the **CRA should reflect the customer's nature and way of business at the obliged entity**, while the **ERA should reflect the obliged entity's nature and business**.

Obliged entities referred to in point 1 of Section 1.2 of the guidelines that have branches and subsidiaries under majority ownership are also required to formulate a group ERA, taking account of the ERAs of the individual undertakings making up the group. Obliged entities that are part of a group take account of the parent undertaking's ERA.

Obliged entities referred to in point 1 of Section 1.2 of the guidelines define and document the methodology for drawing up the ERA, and also performed **ERA** 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 ERA and the internal policies referred to in the previous paragraph must be **approved by the obliged entity's senior management**.

2.2. 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/FT techniques and trends;
- the obliged entity's internal environment.

Accordingly obliged entities referred to in point 1 of Section 1.2 of the guidelines are required to provide regular review and update of the ERA and the CRA internal policies, including the risk criteria affecting the CRA. In so doing obliged entities must provide for the following at least:

a) the updating of the **ERA 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 ERA, the CRA methodology and the risk criteria in the wake of any significant change (e.g. the introduction of a new product, business practices, distribution channels, new technologies, or organisational changes). An update is not required if the obliged entity assesses that the impact of the change is insignificant for the ERA, the CRA methodology and the risk criteria.

3. Entity's risk assessment

(ERA)

The entity's risk assessment (ERA) **helps the obliged entity in understanding which business lines are exposed to higher risk of potential abuse from the perspective of ML/FT, and in which business lines it is necessary to strengthen the control environment to successfully manage ML/FT risks.** In its Guidelines on sound management of risks related to money laundering and financing of terrorism,[1] the BSBS also states that effective management of ML/FT 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 13 of the ZPPDFT-1 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 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), the effective definition and assessment of individual risks referred to in Article 13 of the ZPPDFT-1 requires obliged entities referred to in point 1 of Section 1.2 of the guidelines to define and assess the risk to the obliged entity, within the framework of which they take account of the attributes of the obliged entity and its operations.

The ERA is used for the following purposes:

- an aid to the obliged entity's senior management in determining whether an effective system of ML/FT 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/FT risks (e.g. renewal of AML/CFT policies and procedures, ensuring adequate human resources, allocating appropriate assets, ensuring a technological upgrade).

In the ERA 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 ERA, such as national risk asessment, sectoral risks and the obliged entity's future strategy (*e.g. expansion of the business network, new products, recruitment*).

The preparation of the ERA methodology and the execution of the ERA itself actively involves the AML/CFT officer, who has the requisite information and professional expertise to assess whether the ERA accords with the nature and scale of the obliged entity's operations. An important role is also played by the individual organisational units at the obliged entity, which in accordance with the ZPPDFT-1 are required to provide support and assistance to the obliged entity in providing the needed information and documentation for the ERA. When the obliged entity assigns the preparation of the ERA 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 ERA and the information that formed the basis for its preparation, and to assess whether the ERA presents a true picture of the situation at the obliged entity.

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

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

3.1. ERA methodology

The ERA must encompass the obliged entity's operations in their entirety, i.e. the organisational units and business lines where the obliged entity is exposed to ML/FT risks. The ERA 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**.

<table>
<tr><th colspan="3">OBLIGED ENTITY'S RISK ASSESSMENT</th></tr>
<tr><th>Inherent risk</th><th>Control environment</th><th>Residual risk</th></tr>
<tr><td>Customers</td><td>ML/FT risk management</td><td rowspan="10">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</td></tr>
<tr><td></td><td>Policies and procedures</td></tr>
<tr><td>Geographical regions</td><td>Customer due diligence</td></tr>
<tr><td></td><td>Reporting</td></tr>
<tr><td>Products and services</td><td>Record-keeping and data retention</td></tr>
<tr><td></td><td>AML/CFT function</td></tr>
<tr><td>Transactions</td><td>Identification and reporting of suspected ML/FT</td></tr>
<tr><td></td><td>Monitoring and controls</td></tr>
<tr><td>Distribution channels</td><td>Training</td></tr>
<tr><td></td><td>Independent auditing</td></tr>
<tr><td>Other risks</td><td>Supervisory measures</td></tr>
</table>

The ERA depends on the size of the obliged entity, the nature of its operations and its risk appetite policy, and consequently on the controls put in place with regard to risks.

The **criteria for assessing inherent risk and the areas based on which obliged entities assess the control environment** and that must be taken into account by obliged entities as a minimum standard 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/FT risks.

3.1.1. 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:

- **Risk criteria related to the customer**

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/FT in respect of the customer*).

- **Risk criteria related to the geographical region**

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 residence (*e.g. number of customers that have a registered office or permanent 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 permanent 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*).

- **Risk criteria related to the Product/service/transaction**

The products, services and transactions that the obliged entity offers to customers may have a material impact on ML/FT 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. value 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 Western Union / MoneyGram services; trade credits; 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*).

- **Risk criteria related to distribution channels**

Certain distribution channels pose a higher ML/FT risk, and therefore should reasonably be taken into account 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, through video identification, via an agent*).

- **Other risks**
  - 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 method of business, the inherent risk is determined for each business line, namely for **Personal banking** (natural persons), **Private banking** (legal and natural persons to whom the obliged entity offers individual treatment and special business terms, see also *Section 1.3 Definition of terms*), **SME business line** (legal and natural persons engaging in activities on the market, e.g. enterprenuers), **Corporate banking** (large enterprises that are not covered by any of the aforementioned business lines), **Correspondent banking** (banks and other financial institutions with which the obliged entity has entered into a

correspondent business relationship), and **Investment banking** (financial institutions, legal and natural persons to whom the obliged entity offers investment advice and services).

Such devision 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/FT risks identified through measures that suit the individual business line's way of doing business.

In the ERA the obliged entity takes account of the risk criteria cited above, at a minimum, and also those that could have an impact on its exposure to ML/FT 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
Medimu risk	2
Increased risk	3
High risk	4

The risk criteria described above and the Bank of Slovenia methodology for assessing inherent risk are illustrated in detail in Appendix 1 of the guidelines. Obliged entities may draw up their own methodology for assessing inherent risk, or may apply the Bank of Slovenia methodology as one of the possible approaches to preparing the ERA. In so doing, the obliged entity is required to apply the Bank of Slovenia methodology such way that the ERA reflects the specific attributes of obliged entity's operations.

3.1.2. 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 department), 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:

- **ML/FT risk management**

The senior management is responsible for putting in place an effective risk management system 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/FT risks are put in place, the proper positioning of the AML/CFT function in the bank's organisational structure, whether the AML/CFT function is recognised as a key function*).

- **Policies and procedures**

Review if obliged entity's internal policies are in compliance with the law requirements and the competent supervisory authorities guidelines. Within the framework of the ERA 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 issued by competent authorities, whether the obliged entity has implemented the policies of the group in timely manner*).

- **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 identified deficiencies properly managed (*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 bank's organisational structure (as defined in the point 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 control environment assessment , 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 execution AML/CFT tasks (*e.g. frequency of reporting by business units to the AML/CFT officer*) or supervision of the performance of AML/CFT tasks (*e.g. frequency of reports by business line AML/CFT coordinators*).

- **Record-keeping and data retention**

The obliged entity assesses whether records 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 kept. 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 retention of data obtained during customer due diligence; adequacy of data records 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 employees performing such tasks in addition to their regular work (deputies, business line AML/CFT 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 business line AML/CFT coordinators perform their work effectively and with the requisite quality*).

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

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 to the FIU (*e.g. adequate functioning of software support for identifying unusual transactions, adequate treatment of of alerts, timely reporting to the AML/CFT officer or the FIU*).

- **Monitoring and internal controls**

The obliged entity is required to provide 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 department 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**

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, elimination of breaches*).

- **Supervisory measures**

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

In analysing the control environment the obliged entity takes account of the areas cited above at a minimum, and the risk criteria that it judges have an impact on its ML/FT 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 areas and risk criteria described above and the Bank of Slovenia methodology for assessing the control environment are illustrated in detail in Appendix 1 of the guidelines. Obliged entities must draw up their own methodology for assessing the control environment, or may apply the Bank of Slovenia methodology as one of the possible approaches to preparing the ERA. In so doing, the obliged entity is required to apply the Bank of Slovenia methodology such that the ERA 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 ERA 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.

3.1.3. 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/FT, 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				
	Increased				
	Medium				
	Low				

The AML/CFT officer may propose that the residual risk assessment be raised or lowered by a maximum of one level (*e.g. a planned 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 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.

When preparing the methodology for assessing residual risk, the obliged entity may take account of the Bank of Slovenia methodology for the residual risk assessment, which is given in Appendix 1 of the guidelines.

3.2. Obliged entity's measures on the basis of the ERA

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

1. **The obliged entity documents the ERA**: 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 ERA 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 ERA to the persons responsible** for individual business lines and to the **internal audit department**.
4. On the basis of the ERA, the obliged entity draws up **ML/FT risk management measures** as illustrated below.

On the basis of the level of residual risk identified within the framework of the ERA, the obliged entity draws up measures to mitigate any ML/FT 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 alerts for unusual transactions*) were identified during the ERA, it is necessary to draw up an **action plan for the elimination of the identified deficiencies, and to set a deadline by which the deficiencies must be eliminated**. Identified deficiencies must be eliminated by a reasonable deadline, or by no later than the time of the next ERA.

The residual risk level in the ERA 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 ERA findings.

The ERA 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.

4. Customer risk assessment
(CRA)

Based on the customer risk assessment (CRA), the obliged entity determines the type of due diligence (enhanced, simplified, standard) and the scope and frequency 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.

To be able to undertake the CRA in the area of ML/FT risks it is necessary to:

- identify the risk criteria, and
- determine 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/FT risks** that entail a minimum standard.

Risk criterion risk level
Low risk
Medium risk
Increased risk
High risk

The obliged entity may take account of additional risk criteria, or may treat them more strictly than defined in the guidelines. Because of the risk-based approach in the CRA, an individual risk criterion does not yet necessarily mean the allocation of the customer to a low risk customer risk category or high risk, unless this is explicitly stipulated in the ZPPDFT-1 and the guidelines (a high-risk risk criterion automatically assigns the customer to the customer risk category of high risk).

4.1. 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.

4.1.1. Customer risk

Customer risk is the risk inherent in:

- the **customer's activities**, which is closely related to the monitoring of the purpose and scopefo 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, either on the basis of publicly available data (*from the media, information from other sources, where the assessment of this information should also take account of the reliability and credibility of the source, e.g. articles about the final conviction of person X for the criminal offence of money laundering or an economic crime are considered negative information, while information from forums about the alleged actions of person X is not*), or on the basis of internal information (*e.g. the customer committed fraud in relation to 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 requested evidence*).

The obliged entity also takes account of **risks in connection with parties related to the customer** (statutory representatives, persons with power of representation, beneficial owner).

The set of **customer-related 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.

CUSTOMER LEGAL/NATURAL PERSON	CUSTOMER-RELATED RISK CRITERIA	RISK LEVEL
NP	The customer's identity was verified on the basis of a temporary residence permit or an asylum-seeker's ID card	
NP	The customer, its statutory representative or its person with power of representation is a PEP, an immediate family member of a PEP, or a close associate of a PEP	
NP/LP	The customer is a resident	
NP/LP	The customer is a non-resident	
NP/LP	Negative information has been obtained in connection with the customer, its statutory representative, its person with power of representation or the beneficial owner	
NP/LP	Indicators of suspected ML/FT 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	
NP/LP	The customer, its statutory representative, the person with power of representation or the beneficial owner has been reported to the FIU for suspected ML/FT	
NP/LP	The FIU has submitted a request for ongoing monitoring of a customer's financial transactions or an order for temporarily suspending a transaction	
NP/LP	An enquiry has been received from the FIU for the customer, its statutory representative, the person with power of representation or the beneficial owner	
LP	An undertaking listed on a securities market to which disclosure requirements and requirements for adequate transparency of the beneficial owner apply	
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	
LP	Public administration bodies and public enterprises in Slovenia	
LP	Undertaking under 100% ownership of the Republic of Slovenia	
LP	Undertakings operating in the following industries or whose business activities are as follows: • 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; • 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.).	
LP	The undertaking's ownership structure is unusual or overly complicated relative to the nature of its business	
LP	Sudden changes in the ownership structure or ultimate beneficial owner that cannot be explained	
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	
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	
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)	
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 elimination of breaches in the area of AML/CFT or administrative fines have been imposed on it by supervisory authorities	
LP	The statutory representative, person with power of representation or beneficial owner is a PEP, an immediate close family member of a PEP, or a close associate of a PEP	
LP	The legal person has been established in favour of a PEP, or the statutory representative, person with power of representation or beneficial owner is a foreign PEP	
LP	Other undertakings that are not assessed as high-risk or low-risk	

4.1.2. 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 permanent and temporary residence;
- for legal persons, the registered office as evident from the business register;
- for the statutory representative, the person with power of representation and the beneficial owner, the nationality and the region of permanent 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.

CUSTOMER LEGAL/NATURAL PERSON	COUNTRY RISK CRITERIA	RISK LEVEL
NP/LP	The customer, statutory representative, person with power of representation or beneficial owner 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)	
NP/LP	The customer, statutory representative, person with power of representation or beneficial owner has a registered office or permanent 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)	
NP/LP	The customer, statutory representative, person with power of representation or beneficial owner is a national of a country that is assessed as an **medium risk** (the country is not assessed as a low, increased or high risk)	
NP/LP	The customer, statutory representative, person with power of representation or beneficial owner has a registered office or permanent or temporary residence in a country that is assessed as an **medium risk** (the country is not assessed as low, increased or high risk)	
NP/LP	The customer, statutory representative, person with power of representation or beneficial owner is a national of a country that is assessed as **increased ML/FT risk** (countries where there is higher probability of money laundering or terrorist financing; countries against which restrictive measures have been imposed by the UN Security Council or the EU)	
NP/LP	The customer, statutory representative, person with power of representation or beneficial owner has a registered office or permanent or temporary residence in a country that is assessed as **increased ML/FT risk** (countries where there is a higher probability of money laundering or terrorist financing; countries against which restrictive measures have been imposed by the UN Security Council or the EU)	
NP/LP	The customer, statutory representative, person with power of representation or beneficial owner is a national of a country that is on the **list of high-risk third countries**	
NP/LP	The customer, statutory representative, person with power of representation or beneficial owner has a registered office or permanent or temporary residence in a country that is on the **list of high-risk third countries**	
NP/LP	The customer, statutory representative, person with power of representation or beneficial owner has a registered office or residence at an address that is known to be fictitious (including PO boxes in the rest of the world)	

Having regard for the ML/FT 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-1. Obliged entities assess an individual geographical region as a **low risk, medium risk, increased risk or high risk**.

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

- the list of countries published by the FIU on its website in accordance with the ZPPDFT-1, including:
  - high-risk third countries with strategic deficiencies where adequate AML/CFT measures are not applied;
  - countries where there is a higher probability of money laundering or terrorist financing;
- countries against which restrictive measures have been imposed by the UN Security Council or the EU.[2]

[2] In connection with lists of restrictive measures, the use of the EU Sanctions Map is recommended (https://sanctionsmap.eu/#/main).

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 Office 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. reports 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 about the use of fictitious addresses*).

4.1.3. 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 beneficial owner 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 repayments 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- and 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. 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/FT risk: • mortgage loans; • other purpose-specific 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/FT risk.	
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; • products related to virtual assets; • other products that the obliged entity has assessed as posing increased ML/FT risk.	
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); • Western Union, MoneyGram; • services related to virtual assets; • other services that the obliged entity has assessed as posing increased ML/FT risk.	
NP/LP	Products and services that the obliged entity has assessed as posing medium 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: • 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 on 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 bank and the registered office of the customer, frequent and unexplained transfers of funds to different geographical regions); • transactions with countries on the list of countries that pose increased ML/FT risks; • transactions related to countries on the list of high-risk third countries.	

4.1.4. Risks related to distribution channels

In this case there is an assessment of in what way does the distribution channel, via which the obliged entity offers products or services to the customer, present the risk of misuse for ML/FT purposes. 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.

CUSTOMER	DISTRIBUTION CHANNEL RISK CRITERIA	RISK LEVEL

LEGAL/NATURAL PERSON		
NP	The product or service is offered by means of video-based electronic identification (Article 27 of the ZPPDFT-1)	(at least 1 year)
NP/LP	The product or service is offered in the personal presence of the customer or the statutory representative	
NP/LP	The business relationship is entered into via a person with power of representation	
NP/LP	The business relationship is entered into via an agent/intermediary	
NP/LP	The business relationship is entered into on the basis of electronic means of identification (Article 26 of the ZPPDFT-1)	
NP/LP	The business relationship is entered into via a third party	

4.2. CRA methodology

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

- appropriately **evaluate the aforementioned risk criteria** (that exist at the obliged entity), whereby they must have at a minimum the level of risk defined as 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.

The **Bank of Slovenia methodology for the CRA** is given in **Appendix 2** of the guidelines, **as an aid to obliged entities**. Obliged entities may use it in full or in part, or may use their own CRA methodology to formulate CRAs.

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[3]	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

4.3. Definition of initial CRA and updating of CRA

The obliged entity is required to conduct customer due diligence before entering into a business relationship, and obtain, at a minimum, information set out by the ZPPDFT-1 (*e.g. the customer's registered office or permanent residence, nationality, information about PEPs*). Based on the information obtained about the customer, the 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, and later also the **frequency of transaction monitoring** and the **frequency of reviewing and updating the information and documentation about the customer**, and determines the initial customer risk category.

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, on a basis 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/FT risk than was evident from the information obtained when the business relationship was entered into. In general these are cases when the bank 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/FT 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/FT risks, information about the customer risk category must be available at any time to employees at the obliged entity whose work duties involve ML/FT risk management. Accordingly obliged entities referred to in point 1 of Section 1.2 of the guidelines are **expected to manage the information on customer risk category in their IT support**, which allows proper traceability of changes to the initial CRA.

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 referred to in point 1 of Section 1.2 of the guidelines are therefore recommended to **put in place IT support that provides automatic execution of the CRA and application of the customer risk category to the customer**. The system must also allow manual changes to the automatically applied customer risk category. The grounds for any manual change and

[3] Irrespective of the customer risk category, the obliged entity should ensure that individual high-risk transactions, based on the requirements of the ZPPDFT-1 or the obliged entity's own assessment, are monitored as they happen: for more detailed information, see *Section 4.6 Transaction monitoring*.

information about the employee who entered the change in customer risk category must be recorded.

4.4. Scope of due diligence with regard to CRA

Based on the customer risk category, the obliged entity determines the scope of customer due diligence, which includes the process of obtaining information about the customer, the frequency of transaction monitoring, and the frequency of reviewing and updating 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/FT risks** on the basis of the risk criteria.

The CRA methodology must include risk criteria that will identify customers that pose **high ML/FT 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/FT 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-1 and the guidelines, obliged entities define **measures of standard, simplified and enhanced due diligence in detail in their internal policies and instructions**.

4.4.1. Standard due diligence

In customer due diligence, the obliged entity reliably determines and verifies the customer's identity, and establishes the purpose of a 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/FT.

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 determines and obtains the information about the **beneficial owner** required by law;
- it obtains information about the **purpose and intended nature** of the business relationship or transaction;
- it verifies and determines the **customer's political exposure**.

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**.

4.4.2. 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, except that the measures may be slightly simplified, which allows for the following:

- a **reduced set of information** about the customer, the statutory representative, or the person with power of representation;
- **information on the purpose and intended nature of the business relationship** is only required if it is not evident from the business relationship itself (*e.g. purpose-specific loans, deposits*);
- a **lower frequency of transaction monitoring (annual)**; and
- a **longer period for reviewing and updating information and documentation** about the customer **(three to five years)**.

The aforementioned simplified due diligence measures apply to natural and legal persons, and to the latter in addition:

- **simplified review of the statutory representative or person with power of representation**: when in accordance with the ZPPDFT-1 the obliged entity obtains information by viewing the original or a certified copy of documentation from a relevant register or by viewing the register directly, there is **no need** for the statutory representative or the person with power of representation to **be present in person**;
- **simplified review of the beneficial owner**: the obliged entity obtains the information about the beneficial owner required by law on the basis of a declaration by the statutory representative or the person with power of representation, and not by viewing the original or a certified copy of documentation from a relevant register or by viewing the register directly.

4.4.3. 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 to managanage the risks posed by customers and business relationships that in accordance with the CRA and the CRA methodology require enhanced due diligence.

The obliged entity's CRA methodology should ensure that enhanced due diligence is always conducted in cases set out by the **ZPPDFT-1**, i.e. in the following cases:

- a **correspondent banking relationship** with a bank or similar credit institution established in a third country;
- a business relationship with a **PEP**;
- a business relationship with a **customer linked to a country that is on the list of high-risk third countries**;
- a business relationship entered into by means of **video-based electronic identification**;
- a business relationship in which the obliged entity has identified **increased ML/FT risk on the basis of the risk assessment**.

When conducting enhanced due diligence, the obliged entity takes account of the enhanced due diligence measures required by the ZPPDFT-1. When the ZPPDFT-1 does not set out enhanced due diligence measures, but the obliged entity has identified increased or high ML/FT 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;
- collection of information on the **source of funds and source of wealth**: 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*);
- **approval** of the business relationship by a **responsible person in a senior management position**;
- **assessment** of the compliance of the business relationship **by the AML/CFT department** (*in exceptional cases when professional judgement and assessment of ML/FT risks are required: e.g. entering into business relationships with customers on lists of restrictive measures, PEP monitoring*);
- **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 of reviewing and updating information and documentation about the customer[4] are mandatory elements of enhanced due diligence** (unless stipulated otherwise by the ZPPDFT-1 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/FT risks, in addition to the measures cited above, the obliged entity may also carry out other enhanced due diligence measures.

4.4.3.1. Features of enhanced due diligence for PEPs

PEPs pose a high ML/FT 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, colleagues, or other legal and natural persons. For this reason the ZPPDFT-1 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 on wealth and information on the source of the funds with which the customer will do business via the obliged entity;
- 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 client's other business activities.

Review of political exposure

Under the ZPPDFT-1 obliged entities are required to define the procedure by which they determine whether a customer, its statutory representative, its person with the power of representation or its beneficial owner is a PEP. To this end, obliged entities referred to in point 1 of Section 1.2 of the guidelines are required in accordance with these guidelines to implement

[4] Article 49 of the ZPPDFT-1 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 fourth 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/FT 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.

automatic PEP screening procedure to determine the political exposure of customers and related parties using commercial PEP databases.

The procedure for determining whether a customer is a PEP is required before the business relationship is entered into, and during the business relationship. Obliged entities are required to review the political exposure of customers **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 owned by the government*), 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 automatic PEP screening procedure in place have to review their existing customer base whnever there is a change in the customer information of if there were any changes on the PEP list in the 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 also taken into account in the CRA.

Not all PEPs pose the same ML/FT 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, his/her statutory representative or the person with power of representation is a PEP**, it is required to carry out enhanced due diligence measures as cited by the ZPPDFT-1, and to place the customer into a customer risk category that is the same as or comparable to the customer risk category of high risk as set out by the Bank of Slovenia methodology.

When entering into business relationships with **legal persons**, the obliged entity must also check any political exposure of the **statutory representative, the person with power of representation and the beneficial owner**. The scope of the enhanced due diligence applying to PEPs in these cases relates to the **legal person**, whereby it is necessary to take account of the following features with regard to enhanced due diligence measures:

a) The obliged entity is entering into a business relationship with a **legal person that is under majority government ownership, with diplomatic or consular representative offices or other government or international institutions defined in the ZPPDFT-1**, whereby their statutory representatives are PEPs on account of their function alone (*e.g. ambassador, CEO of an enterprise under majority government ownership*):
    - *Customer risk category:* In these cases the obliged entity takes account of the information about PEP status 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.
    - *Scope of due diligence and transaction monitoring:* The scope of customer due diligence and the frequency of transaction monitoring are determined in accordance with the customer risk category: simplified, standard or enhanced due diligence, monthly, half-yearly, annual.
    - *Measures:* The obliged entity obtains written approval from a superior responsible person in a senior management position, and the AML/CFT officer's opinion with regard to the appropriateness of the customer risk category.

b) The obliged entity is entering into a business relationship with a **legal person whose statutory representative, person with power of representation or beneficial owner is a PEP**, or that is **known to be a legal person established in favour of a PEP**.
   - *Customer risk category:* The obliged entity is required to place the customer into a customer risk category that is the same as or comparable to the customer risk category of high risk as set out by the Bank of Slovenia methodology.
   - *Scope of due diligence and transaction monitoring:* The obliged entity is required to conduct enhanced due diligence (Section 4.4.3 Enhanced due diligence) and to conduct transaction monitoring on a monthly basis (Section 4.6 Transaction monitoring).
   - *Measures:* The obliged entity obtains information on wealth and information on the source of the funds with which the customer will do business via the obliged entity (i.e. the legal person), and written approval from the superior responsible person in a senior management position.

c) The obliged entity is entering into a business relationship with **legal persons whose statutory representative, person with power of representation or beneficial owner is a foreign PEP**.
   - *Customer risk category:* The obliged entity is required to place the customer into a customer risk category that is the same as or comparable to the customer risk category of high risk as set out by the Bank of Slovenia methodology.
   - *Scope of due diligence and transaction monitoring:* The obliged entity is required to conduct enhanced due diligence (Section 4.4.3 Enhanced due diligence) and to conduct transaction monitoring on a monthly basis (Section 4.6 Transaction monitoring).
   - *Measures:* The obliged entity obtains information on wealth and information on the source of the funds with which the customer will do business via the obliged entity (i.e. the legal person), written approval from the superior responsible person in a senior management position, and an opinion from the AML/CFT officer assessing whether the reasons for which the foreign PEP is entering into a business relationship via the legal person and outside the country in which he/she holds a political function pose potential ML/FT risks.

Collection of information about the source of funds and wealth

When 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 related party. Information about the **source of wealth** is obtained from public records or documents and other documentation submitted to the obliged entity by the customer or, where this is not possible, from the customer's written declaration.[5] Information about the **source of funds** is obtained directly from the customer, as it has an impact on the purpose and scale of the customer's business with the obliged entity.

Existing customer

When an existing customer, the statutory representative, the person with power of representation or beneficial owner becomes a PEP during the business relationship (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 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;

[5] 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/Pregled-stranke/ugotavljanje_in_preverjanje_istovetnosti_tujcev.pdf

- 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 position**;
- the **transaction monitoring of the PEP is monthly**, or as described in detail below (see *Transaction monitoring of PEPs*).

Transaction monitoring of PEPs

The fact that the customer's risk level has changed has an impact on the frequency of transaction monitoring. As stated in *Section 4.6 Transaction monitoring*, the transactions of high-risk customers (including PEPs) are monitored at least monthly.

If the obliged entity assesses that the transactions of a customer who is a PEP or of related parties **do not deviate from the stated purpose and scale of transactions**, or the **obliged entity assesses that the customer's transactions pose no ML/FT 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 employees at the obliged entity of any deviations from the purpose and scope of transactions;
- an opinion has been obtained from the AML/CFT department; and
- the decision has been approved by the superior responsible person in a senior management position.

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 an medium risk before acquiring PEP status.

A customer who is a PEP or whose related party 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 Bank of Slovenia methodology**, as a minimum legal requirement. 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.

4.4.3.2. 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 system. The list is published by the *FIU* on its website[6] (List of high-risk third countries).

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

Under the ZPPDFT-1 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 to a high-risk third country when:

- he/she is a national of a country that is on the list of high-risk third countries;
- it has a registered office or he/she has permanent or temporary residence in a country that is on the list of high-risk third countries;

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

- the statutory representative, person with power of representation or beneficial owner is a national of a country that is on the list of high-risk third countries;
- the statutory representative, person with power of representation or beneficial owner has permanent 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 of:

- 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;
- the 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 position;
- more frequent transaction monitoring; and
- a shorter period for reviewing and updating information and documentation about the customer.

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

If the customer or the statutory representative, person with power of representation or beneficial owner 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 4.1.2 Country risk*).

Transaction monitoring 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 4.6 Transaction monitoring*).

If the obliged entity judges that the transactions of a customer who has a registered office or residence 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/FT 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 department; and
- the decision has been approved by the superior responsible person in a senior management position.

A customer who has a registered office or residence 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 Bank of Slovenia**

methodology, as a minimum legal requirement. 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.

Review of transactions linked to the list of high-risk third countries

The ZPPDFT-1 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.

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:

- within the transaction monitoring of the customer, the obliged entity judges whether transactions with countries on the list of high-risk third countries accord with the purpose, nature and scope 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 with such countries;
- any transaction in exceeding EUR 15,000 that is executed at the customer's request onto the accounts of legal or natural persons in a country on the list of high-risk third countries or onto accounts of legal and natural persons that have a registered office or permanent or temporary residence in a country on the list of high-risk third countries, obliged entity must report to the *FIU* ;
- in the event of the identification of suspicious customer behaviour or in connection with suspicious transactions 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 Bank of Slovenia methodology, and assesses whether the suspected ML/FT should be reported to the *FIU*.

Occasional transactions

The ZPPDFT-1 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 that exceeds EUR 1,000, customer due diligence is required by law.

If an occasional transaction that requires customer due diligence under the ZPPDFT-1 is ordered by a person with links to a country that is on the list of high-risk third countries, the obliged entity must obtain information about the reasons for the intended occasional transaction.

The obliged entity is also required to gather information about the reasons for an intended occasional transaction when it has been executed onto the accounts of legal or natural persons in a country on the list of high-risk third countries or onto the accounts of legal and natural persons that have a registered office or permanent or temporary residence in a country on the list of high-risk third countries.

Payment transactions

As an additional measure of enhanced due diligence in the case of transactions 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 simultaneously payment institutions ensure that transactions are always accompanied by information about the purpose of the transaction.

4.5. Prohibited transactions

Article 64 of the ZPPDFT-1 prohibits the **use of anonymous products** that could directly or indirectly allow the concealment of the customer's identity, which obliged entities must take into account when assessing the risk of a new product or service.

The ZPPDFT-1 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 Bank of Slovenia 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 an 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 correspondence key, obliged entities that have correspondent relationships or accounts with banks are required to verify whether the bank is acting as a shell bank or does business with banks of this type.

4.6. Transaction monitoring

Transaction monitoring differs with regard to customer risk category: under the ZPPDFT-1 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, while less frequent monitoring is allowed 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 customer risk category of the customer executing the transaction):

- transactions referred to in Article 68 of the ZPPDFT-1, irrespective of whether the customer appears in the role of payer or payee;
- transactions on a previously dormant account;
- other high-risk transactions that the obliged entity assesses as requiring daily monitoring.

With regard to the risk criteria deriving from the customer's transactions themselves (or an individual transaction), the obliged entity must also provide for the **regular updating of the CRA**. Irrespective of the envisaged period for customer due diligence follow-up, the obliged entity must update the CRA whenever it identifies any suspected ML/FT in connection with the customer or a

transaction, and whenever it establishes during the customer's transactions that a risk criterion is assessed as a high risk in line with its CRA methodology (*e.g. the customer is a PEP, a report of suspected ML/FT 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. Obliged entities referred to in point 1 of Section 1.2 of the guidelines are expected to put in place IT support for transaction monitoring such that risk criteria deriving from the customer's transactions (or an individual transaction) enable the automatic updating of the (initial) CRA and the customer risk category. The system must also allow manual changes to the 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.

4.7. Review and updating of information and documentation

Under the ZPPDFT-1 obliged entities are required to review and update the information and documentation obtained about the customer, whereby the obliged entity alignes the scope and frequency to the ML/FT risks identified on the basis of the risk assessment, or undertakes review and updating no more 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 scope of the transactions and whether the customer has become a PEP**. With regard to the checks carried out, the obliged entity updates the information and the CRA as necessary, and keeps an appropriate record customer due diligence follow-up.

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/FT 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 an **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.

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 sets limitations for 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 that require customer due diligence[7] in accordance with the ZPPDFT-1.**

The obliged entity may also apply the aforementioned measures to customers that it assesses a 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 such limitations; transactions for which customer due diligence is not required under the ZPPDFT-1 are also not subject to limitations.[8]

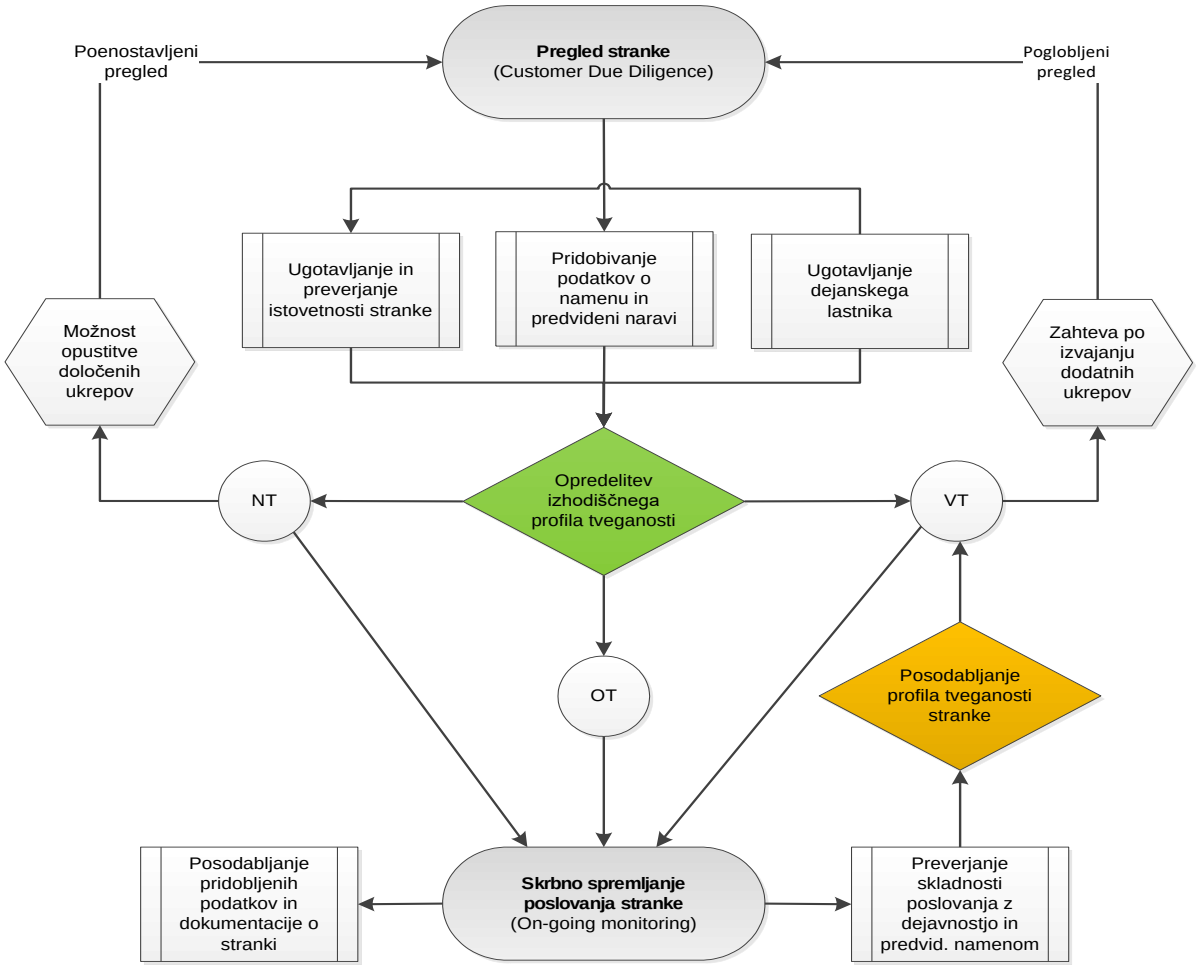
In any case, the **customer's lack of response to the obliged entity's call to submit the information and documentation required to carry out the updating required by law needs to be assessed from the perspective of ML/FT risks**, and within this framework there is also a need to assess whether it is reasonable to make a suspicious transaction report to the FIU, and whether it is reasonable to continue the business relationship with the customer.

If a customer fails to execute a single transaction during a period of more than 12 months, i.e. there is a **dormant account** (interest and account management costs are not counted as customer transactions), there is no need for transaction monitoring or the review and updating of the information and documentation about the customer. In these cases the obliged entity ensures 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 customer due diligence is follow-up is performed, 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 risk criteria related to products, services and transactions.

Process of defining initial CRA and updating CRA:

[7] Any transaction in the amount of EUR 15,000 or more (irrespective of whether executed individually or in several evidently linked transactions) that the customer executed within the framework of an existing business relationship (point 2 of the first paragraph of Article 17 of the ZPPDFT-1).

[8] i.e. transactions not covered by point 2 of the first paragraph of Article 17.


Poenostavljeni pregled
Pregled stranke (Customer Due Diligence)
Poglobljeni pregled
Ugotavljanje in preverjanje istovetnosti stranke
Pridobivanje podatkov o namenu in predvideni naravi
Ugotavljanje dejanskega lastnika
Možnost opustitve določenih ukrepov
Zahteva po izvajanju dodatnih ukrepov
NT
Opredelitev izhodiščnega profila tveganosti
VT
OT
Posodabljanje profila tveganosti stranke
Posodabljanje pridobljenih podatkov in dokumentacije o stranki
Skrbno spremljanje poslovanja stranke (On-going monitoring)
Preverjanje skladnosti poslovanja z dejavnostjo in predvid. namenom

5. Customer acceptance policy

On the basis of the ERA the obliged entity formulates and updates its customer acceptance policy; this document sets out obliged entity **intentions with regard to doing business with customers asper their individual CRAs**.

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/FT risks, a control environment tailored to the lower risks that the obliged entity is willing to take up is allowed.

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 due to the excessive risk that the obliged entity's system could be misused for ML/FT.

6. Final provisions

The guidelines enter into force after their publication on the Bank of Slovenia website.

Obliged entities are required to bring their policies, controls and procedures in line with the guidelines within 12 months of the publication of the guidelines on the Bank of Slovenia website.

Obliged entities referred to in point 1 of Section 1.2 are required to draw up the first CRA in accordance with the guidelines by 31 March 2021.

APPENDIX 1: Bank of Slovenia methodology for the ERA

Priloga 1_Metodologija BS z

APPENDIX 2: Bank of Slovenia methodology for the CRA

Priloga 2_Metodologija BS z

APPENDIX 3: Sectoral guidelines for individual obliged entities

The sectoral guidelines are aimed at individual obliged entities for the purpose of setting out the the guidelines tailored to the specific needs of individual obliged entities, namely:

- **payment institutions and payment institutions with a waiver (that are not banks, savings bank or branches of foreign banks);**
- **electronic money institutions and electronic money institutions with a waiver;**
- **currency exchange offices.**

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 *mutatis mutandis*. Notwithstanding the above, Section 3 of the guidelines (Obliged entity's risk assessment) does not apply to obliged entities referred to in the previous paragraph.

In accordance with the second paragraph of Article 13 of the ZPPDFT-1, obliged entities draw up a risk assessment for an individual group or type of customer, business relationship, transaction, product, service or distribution channel, taking into account the geographical risk factors with respect to potential abuse for the purpose of money laundering and terrorist financing. In the risk assessment of individual groups, types or areas of risk, obliged entities are **recommended** to proportionately apply, *mutatis mutandis*, the risk criteria described by group and area in Section 3 of the guidelines (Obliged entity's risk assessment).

The sectoral guidelines provide detailed regulation of the risk criteria based on which obliged entities assess ML/FT risks within the framework of the customer risk assessment (CRA).

The risk criteria described in the individual sections of the sectoral guidelines are by no means exhaustive. Obliged entities are required to have an overview of risk, and to take account of criteria that they themselves assess as having an impact on the CRA. They may also take account of other criteria cited in the guidelines (in addition to the criteria set as the minimum standard by the sectoral guidelines).

1. Features of risk assessment for payment institutions

The Bank of Slovenia provides more detailed guidance below for obliged entities that are payment institutions and payment institutions with a waiver (and are not banks, savings banks or branches of foreign banks) with regard to individual requirements under the guidelines.

Payment institutions provide payment services, and require the relevant authorisation in accordance with the *law governing payment services, electronic money issuance services and payment systems*. TheML/FT risks inherent from the customers, and from the transactions that customers execute within the business relationship and from occasional transactions as defined by the ZPPDFT-1.

1.1. CRA risk criteria

The set of 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 (defined in the guidelines or derived from the obliged entity's way of business) or treat the below criteria more strictly.

CUSTOMER-RELATED RISK CRITERIA	RISK LEVEL
The customer's identity was verified on the basis of a temporary residence permit or an asylum-seeker's ID card	
The customer, its statutory representative or its person with power of representation is a PEP, an immediate family member of a PEP, or a close associate of a PEP	
The customer is a resident	
The customer is a non-resident	
Indicators of suspected ML/FT have been identified 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).	
The customer, its statutory representative, the person with power of representation or the beneficial owner has been reported to the FIU for suspected ML/FT	
The FIU has submitted a request for ongoing monitoring of a customer's financial transactions or an order for temporarily suspending a transaction	
An enquiry has been received from the FIU for the customer, its statutory representative, the person with power of representation or the beneficial owner	
Undertakings whose business activity is highly cash-intensive	
The undertaking's ownership structure is unusual or overly complicated relative to the nature of its business	
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	
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	
The statutory representative, person with power of representation or beneficial owner is a PEP, an immediate family member of a PEP, or a close associate of a PEP	
The legal person has been established in favour of a PEP, or the statutory representative, person with power of representation or beneficial owner is a foreign PEP	
Other undertakings that are not assessed as high-risk or low-risk	

COUNTRY RISK CRITERIA	RISK LEVEL
The customer has permanent or temporary residence in Slovenia or is a Slovenian national	
The customer, statutory representative or person with power of representation has permanent or temporary residence outside Slovenia	
The customer, statutory representative or person with power of representation has permanent or temporary residence in a country that is on the list of high-risk third countries	

Obliged entities 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, obliged entities must always assess and treat geographical regions on the list of high-risk third countries as high-risk geographical regions.

In the risk assessment of geographical regions, obliged entities take account of the following as mandatory resources:

- the list of countries published by the FIU on its website in accordance with the ZPPDFT-1, including:
  - high-risk third countries with strategic deficiencies where adequate AML/CFT measures are not applied;
  - countries where there is a higher probability of money laundering or terrorist financing;
- lists of countries against which restrictive measures have been imposed by the UN Security Council or the EU.

PRODUCT/SERVICE/TRANSACTION RISK CRITERIA	RISK LEVEL
The settlement of liabilities for executed payments and cash withdrawals is executed via current accounts of customers or a payment order at a bank inside the EEA	
Other products/services and transactions that the obliged entity assesses as a low risk	
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.	
Other products/services that the obliged entity assesses as an increased risk	
Transactions that pose an 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; • other transactions that the obliged entity assesses as an increased risk.	

DISTRIBUTION CHANNEL RISK CRITERIA	RISK LEVEL
The product or service is offered by means of video-based electronic identification	(at least 1 year)
The product or service is offered in the personal presence of the customer or the statutory representative	
The business relationship is entered into via a person with power of representation	
The business relationship is entered into via an agent/intermediary	
The business relationship is entered into by means of electronic identification	
The business relationship is entered into via a third party	

2. Features of risk assessment for electronic money institutions

The Bank of Slovenia provides more detailed guidance for obliged entities that are electronic money institutions and electronic money institutions with a waiver (sectoral guidelines) with regard to individual requirements under the guidelines.

ML/FT risks with 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.

2.1. CRA risk criteria

The set of 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 (defined in the guidelines or derived from the obliged entity's way of business) or treat the below criteria more strictly.

CUSTOMER-RELATED RISK CRITERIA	RISK LEVEL
The customer's identity was verified on the basis of a temporary residence permit or an asylum-seeker's ID card	
The customer is a resident	
The customer is a non-resident	
The customer, its statutory representative or its person with power of representation is a PEP, an immediate family member of a PEP, or a close associate of a PEP	
Negative information has been obtained in connection with the customer, the statutory representative or the person with power of representation	
Indicators of suspected ML/FT 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	
The customer, its statutory representative, the person with power of representation or the beneficial owner has been reported to the FIU for suspected ML/FT	
The FIUhas submitted a request for ongoing monitoring of a customer's financial transactions or an order for temporarily suspending a transaction	
An enquiry has been received from the FIUfor the customer, its statutory representative, the person with power of representation or the beneficial owner	

COUNTRY RISK CRITERIA	RISK LEVEL
The customer has permanent or temporary residence in Slovenia or is a Slovenian national	
The customer, statutory representative or person with power of representation has permanent or temporary residence outside Slovenia	
The customer, statutory representative or person with power of representation has permanent or temporary residence in a country that is on the list of high-risk third countries	

Obliged entities 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, obliged entities must always assess and treat geographical regions on the list of high-risk third countries as high-risk geographical regions.

In the risk assessment of geographical regions, obliged entities take account of the following as mandatory resources:

- the list of countries published by the FIU on its website in accordance with the ZPPDFT-1, including:
  - high-risk third countries with strategic deficiencies where adequate AML/CFT measures are not applied;
  - countries where there is a higher probability of money laundering or terrorist financing;
- lists of countries against which restrictive measures have been imposed by the UN Security Council or the EU.

PRODUCT/TRANSACTION RISK CRITERIA	RISK LEVEL
Payment instruments for which the obliged entity has obtained consent from the FIU in accordance with the ZPPDFT-1 to omit certain customer due diligence measures in connection with electronic money	
Other products that the obliged entity assesses as a low risk	
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; • allow 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).	
Transactions that pose an 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 transactions are always just below the thresholds for reporting, etc.; • 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 transactions that the obliged entity assesses as an increased risk.	

DISTRIBUTION CHANNEL RISK CRITERIA	RISK LEVEL
The payment instrument is offered by means of video-based electronic identification	(at least 1 year)
The payment instrument is offered in the personal presence of the customer or the statutory representative	
The business relationship is entered into via a person with power of representation	
The business relationship is entered into via an agent/intermediary	
The business relationship is entered into by means of electronic identification	
The business relationship is entered into via a third party	

3. Features of risk assessment for currency exchange offices

The key risk criteria that raise ML/FT risks at currency exchange offices include widespread cash transactions, the anonymity of transactions, operations at the border areas, and business with occasional customers (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/FT risks.

It should nevertheless be borne in mind that currency exchange operations are not the principal business activity of most currency exchange offices in Slovenia (rather they are engaged in hotel services, retail, food services or hairdressing, for example). The simple nature of their operations (the majority of currency exchange offices are sole traders or micro limited liability companies) should also be noted, as should the fact that in the national ML/FT risks assessment the sector have been identified as low.

The requirements under the guidelines with regard to the **CRA** (Section 4. Customer risk assessment) are not fully binding on currency exchange offices; instead they **apply *mutatis mutandis* only with regard to the scope of customer due diligence** (*see Section 4.4 Scope of due diligence with regard to CRA*). The requirements in connection with customer due diligence at currency exchange offices are presented below.

The requirements of the guidelines with regard to the customer acceptance policy (*see Section 0.*

Customer acceptance **policy**) are also not binding on currency exchange offices.

3.1. Sectoral guidelines with regard to customer due diligence

Under the ZPPDFT-1, when executing currency exchange operations where the transactions exceedes EUR 1,000 the obliged entity is required to conduct customer due diligence, and to:

- establish the customer's identity, and to verify the customer's identity on the basis of credible, independent and objective resources;
- establish the customer's beneficial owner;
- obtain information about the purpose of the transaction.

The obliged entity conducts simplified, standard or enhanced due diligence of the customer with regard to the information obtained and the ML/FT risks identified. The obliged entity takes account of the guidelines when carrying out measures with regard to the scope of due diligence.

The **risk criteria affecting the scope of customer due diligence** with regard to the execution of currency exchange operations are:

CUSTOMER-RELATED RISK CRITERIA	RISK LEVEL
The customer's identity was verified on the basis of a temporary residence permit or an asylum-seeker's ID card	
The customer, its statutory representative or its person with power of representation is a PEP, an immediate family member of a PEP, or a close associate of a PEP	
The customer is a resident	
The customer is a non-resident	
Indicators of suspected ML/FT 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).	
The customer, its statutory representative, the person with power of representation or the beneficial owner has been reported to the FIUfor suspected ML/FT	
The FIUhas submitted a request for ongoing monitoring of a customer's financial transactions or an order for temporarily suspending a transaction	
An enquiry has been received from the FIUfor the customer, its statutory representative, the person with power of representation or the beneficial owner	
Undertakings operating in the following industries or whose business activities are as follows: • 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; • 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.).	
The undertaking's ownership structure is unusual or overly complicated relative to the nature of its business	
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	

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	
The statutory representative, person with power of representation or beneficial owner is a PEP, an immediate family member of a PEP, or a close associate of a PEP	
The legal person has been established in favour of a PEP, or the statutory representative, person with power of representation or beneficial owner is a foreign PEP	

COUNTRY RISK CRITERIA	RISK LEVEL
The customer has permanent or temporary residence in Slovenia or is a Slovenian national	
The customer, statutory representative or person with power of representation has permanent or temporary residence outside Slovenia	
The customer, statutory representative or person with power of representation has permanent or temporary residence in a country that is on the list of high-risk third countries	

Obliged entities 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, obliged entities must always assess and treat geographical regions on the list of high-risk third countries as high-risk geographical regions.

In the risk assessment of geographical regions, obliged entities take account of the following as mandatory resources:

- the list of countries published by the FIU on its website in accordance with the ZPPDFT-1, including:
  - high-risk third countries with strategic deficiencies where adequate AML/CFT measures are not applied;
  - countries where there is a higher probability of money laundering or terrorist financing;
- lists of countries against which restrictive measures have been imposed by the UN Security Council or the EU.

TRANSACTION RISK CRITERIA	RISK LEVEL
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 always just below the thresholds for reporting, etc.; • transactions that do not have a clear economically or legally justified purpose; • 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 residence); • currency exchange into the currencies of countries on the list of high-risk third countries; • other transactions that the obliged entity assesses as an increased risk.	

The **methodology** for the scope of customer due diligence during the execution of currency exchange operations is as follows:

RISK CRITERION RISK LEVEL	SCOPE OF DUE DILIGENCE

Low risk	Simplified
Medium risk	Standard
Increased risk	Standard/enhanced
High risk	Enhanced

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