Guide to the Individual Risk Assessment (IRA)

UIFAND
UNITAT D'INTEL·LIGÈNCIA FINANCERA

July 2018

Table of contents

1. WHAT IS THE INDIVIDUAL RISK ASSESSMENT?

The individual risk assessment (IRA) is a tool conceived to allow each reporting entity to identify and to manage properly the risks of laundering of money or assets and of terrorist financing (ML/TF) to which it is exposed. This assessment should entail a self-assessment process, by each reporting entity, of its own business in order to detect the most vulnerable areas on which the entity should consequently focus the greater part of its control efforts and measures with the aim to reduce the associated risk to an acceptable level according to the tolerance determined by each reporting entity.

Accordingly, the goal of this Guide is to provide reporting entities with some basic guidelines which will allow the performance of an IRA that will cover the real risks to which the entities are exposed.

Although compliance with this Guide is not compulsory, UIFAND considers that the content of this document is relevant for all reporting entities.

2. LEGISLATIVE REFERENTS

The obligation to carry out the IRA is established by **Article 5 of Law 14/2017**:

"1. Reporting entities should adopt suitable measures to identify, assess and understand their risks of laundering of money or assets and of terrorist financing. This individual risk assessment (IRA) should:

a) be properly documented and reflected in a written report;

b) consider all the relevant risk factors before determining the overall risk level and the appropriate mitigating measures. These risk factors should include those relating to customers, countries or geographical areas, products, services, transactions or distribution channels;

c) be updated periodically and in all cases when important events or novelties arise in the reporting entity's governance and activity.

UIFAND may issue guidelines on what suitable measures are considered to be, on the basis of the particularities and size of the reporting entities.

2. The IRA should be made available to UIFAND immediately when it is requested by UIFAND (...)"

Likewise, **Transitory Provision Four** of the aforementioned law establishes the maximum time for the performance of the assessment:

"Reporting entities should carry out their individual risk assessment (IRA) according to the terms provided in Article 5 of this Law, within a time of two years counting from the entry into force of this Law."

In this respect, reporting entities have **until 18 July 2019** to carry out and to document the IRA.

Lastly, the **Regulation of Law 14/2017, in its Article 3,** develops in greater detail the minimum content which the assessment is to contain, as well as other requirements which the reporting entity should fulfil in the internal assessment of its risks:

"1. In application of Article 5 of the Law, when reporting entities identify and assess their risks of laundering of money or assets and terrorist financing, they should consider, among others, the following risk factors:

a) the nature, diversity and complexity of their respective businesses;

b) their target markets;

c) the number of customers and beneficial owners already identified as being of high risk;

d) the jurisdictions to which the reporting entity is exposed, either through its own activity or through the activities of its customers and beneficial owners, especially including the jurisdictions with high levels of corruption or organized crime, and/or deficiencies in the controls of the fight against the laundering of money or assets and terrorist financing indicated by the Financial Action Task Force (FATF);

e) the distribution channels, including the way in which the reporting entity deals with its customers, its level of dependence on third persons for the performance of due diligence measures and its use of technology;

f) the results of the internal audit, if any;

g) the volume and the size of its transactions, considering the usual activity of the reporting entity and the profile of its customers;

h) products and services;

i) the monetary flows with each jurisdiction with which the reporting entity operates, both within the scope of its own activity and within that of the activities of its customers and beneficial owners;

j) the types of companies or entities;

k) the entities or legal structures administered by lawyers, administrative services agents and/or professional providers of services to companies and trusts;

l) the entities or legal structures without apparent economic activity.

2. Reporting entities may supplement this information with information obtained from other pertinent internal or external sources, such as business managers, personal account managers, national risk assessments, lists published by intergovernmental organizations or national governments, assessment reports or reports on types of laundering of money or assets and terrorist financing published by FATF or equivalent bodies such as Moneyval.

3. The individual risk assessment is to be approved by the administration body and it forms the basis for the development of the policies and procedures for mitigating the risks of laundering of money or assets and terrorist financing, because it reflects the risk profile of the reporting entity and determines its level of tolerance. The policies, procedures, measures and controls for mitigating risks should be consistent with the individual risk assessment."

3. WHAT IS THE GOAL OF THE INDIVIDUAL RISK ASSESSMENT?

In order to make compliance with the Regulation of Law 14/2017, the individual risk assessment **should have the minimum content described in the preceding section**, although it should be adapted to the size and characteristics of each business. There is no standard format to be applied.

The ultimate goal of the individual risk assessment is to determine the overall ML/TF risk level of each reporting entity as a whole.

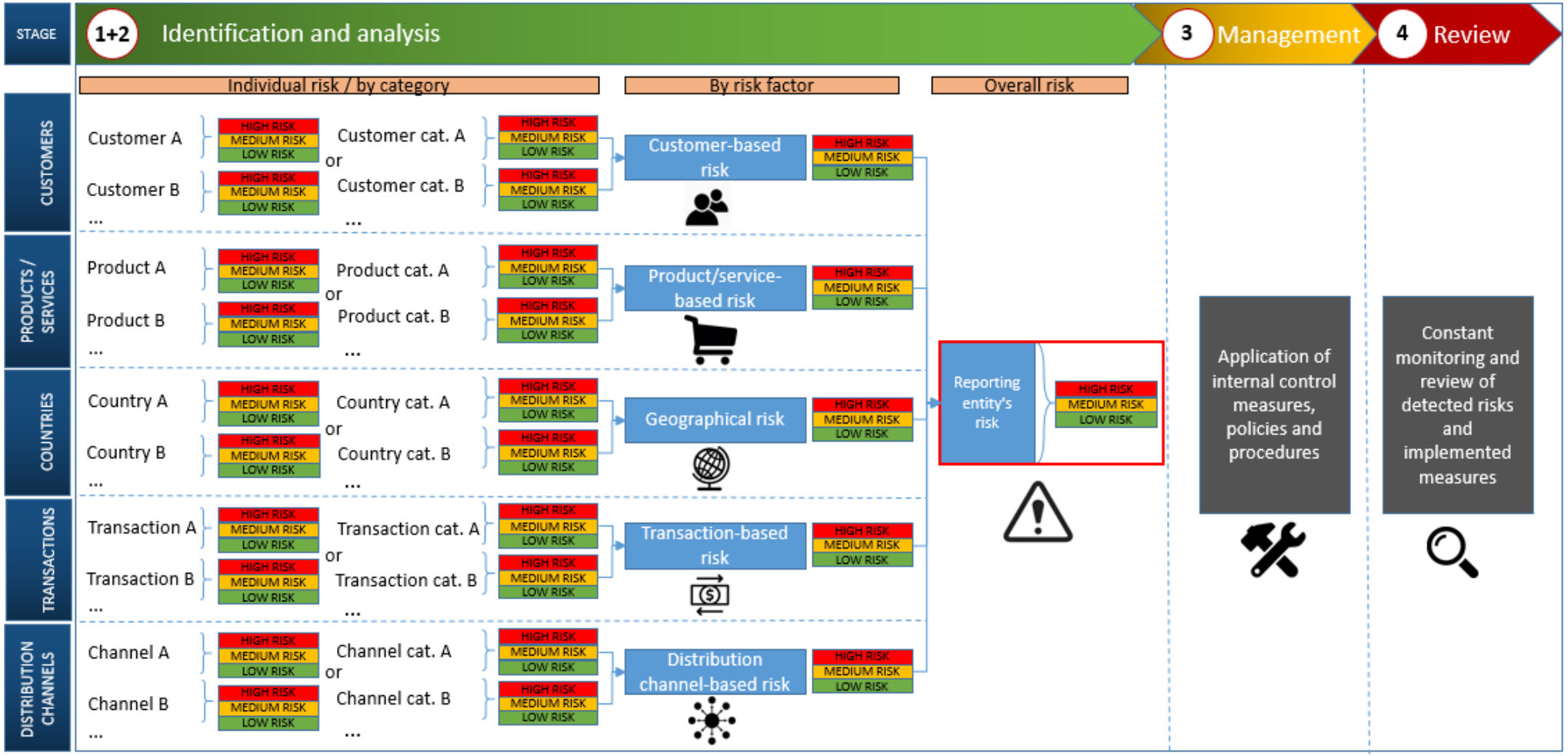
In order to achieve this categorization of the overall risk, it will first be necessary to consider the risk associated with a number of factors, which will vary according to each reporting entity but, in any case, these factors may be grouped into **five major risk factors** which will be described further on.

The IRA is a necessary first step for reporting entities to develop **suitable mitigation and control measures** addressed to dealing with their risks, distributing their resources efficiently in the areas found to present the greatest risk, **consistently with the nature, size and complexity of their business.** Moreover, a **follow-up** and a **monitoring** of the **implementation** of these measures, procedures and controls should be carried out and they should be updated or improved when appropriate.

4. WHAT ARE THE STAGES OF THE INDIVUDAL RISK ASSESSMENT?

An individual risk assessment may be summarized as a self-assessment process formed by the **following four stages**:

1 Identification of risks	Identify the business areas liable to be used for ML/TF, grouped in the following main categories: · Customer-based risk · Product- and service-based risk · Transaction-based risk · Geographical risk · Distribution channel-based risk
2 Analysis of risks	Analyse the detected risks in terms of the probability of their occurrence and their impact in the event of their materialization.
3 Management of detected risks	Apply risk control strategies based on the analysis carried out, and implement fit and proper internal control policies and procedures.
4 Monitoring and review of risks	· Carry out a constant monitoring and review of the detected risks and of the implemented mitigation measures. · Regularly update the individual risk assessment.


STAGE
1+2 Identification and analysis
3 Management
4 Review
Individual risk / by category
By risk factor
Overall risk
CUSTOMERS
Customer A
Customer B
...
HIGH RISK
MEDIUM RISK
LOW RISK
or
Customer cat. A
Customer cat. B
Customer-based risk
PRODUCTS / SERVICES
Product A
Product B
Product cat. A
Product cat. B
Product/service-based risk
COUNTRIES
Country A
Country B
Country cat. A
Country cat. B
Geographical risk
TRANSACTIONS
Transaction A
Transaction B
Transaction cat. A
Transaction cat. B
Transaction-based risk
DISTRIBUTION CHANNELS
Channel A
Channel B
Channel cat. A
Channel cat. B
Distribution channel-based risk
Reporting entity's risk
Application of internal control measures, policies and procedures
Constant monitoring and review of detected risks and implemented measures

5. WHICH RISK FACTORS SHOULD BE CONSIDERED WHEN PREPARING THE IRA?

In **Stage One** of the assessment on the **identification of risks**, the reporting entity should assess the risk of its business being used by criminals for the purpose of concealing the criminal origin of specific funds, laundering the proceeds of crime and/or financing terrorism.

For example, among other cases, (i) the reporting entity may receive funds of criminal origin in accounts which the customer holds in the entity; (ii) the customer may use the reporting entity's services to set up a legal structure that hinders the identification of criminals, or (iii) the reporting entity may be legitimizing funds of criminal origin by participating in the formulation of a company's financial statements which substantiate that such funds are legitimate profits from the company's economic activity, despite the fact that their origin actually has nothing to do with the customer's economic activity.

The risks which reporting entities face, as has been pointed out in the preceding paragraphs, may be grouped into the **following categories or factors**:

- **Customer-based risk**
- **Product- and service-based risk**
- **Geographical risk**
- **Transaction-based risk**
- **Distribution channel-based risk**

The elements to be taken into account for each of these risk factors are dealt with in detail below:

Risk factor 1	**Customer-based risk**

In order to assess the risk associated with this factor, the reporting entity should identify the **type of customers** to whom it provides its services.

In this section, consideration should be given to the classification of each customer according to the level of risk of laundering of money or assets or of terrorist financing which he presents, on the basis of the criteria which the reporting entity shall have defined internally in compliance with the provisions of Article 4 of the Regulation developing Law 14/2017. Moreover, consideration should be given to the percentage of customers who have been classified as of "high risk" with respect to the total number of customers in order to determine the reporting entity's degree of exposure to customer-based risk.

In order to assign the respective risk classification to each customer, consideration should be given to the characteristics of each individual customer or, depending on the volume of customers, the reporting entity may group its portfolio of customers into various categories and determine the associated risk for each category. The following are some examples of such a categorization process:

- According to the **type** of customers (natural persons, legal entities, other legal structures...).
- According to the **corporate format** (public limited company, limited liability company, single-member company...).
- According to **nationality** and **residence.**
- According to **professional activity** or **sector**.
- According to **size** (small companies, multinationals...).
- According to the company's **duration**.
- According to the **length** of the business relation.

With respect to customer-based risk, **Annex I** of this Guide provides some examples of high-risk and low-risk cases.

Risk factor 2	**Product- and service-based risk**

For this risk factor, the reporting entity should **identify all the products and/or services** which it offers and assess the risk which each one poses of being used for the laundering of money or assets or terrorist financing. The risk may be considered for each product or service offered or else the products and services may be grouped into **different areas or lines of business** according to the nature, diversity and complexity of the businesses of each reporting entity.

The reporting entity should also consider the proportion represented by each product, service or area within its overall volume of business. Consequently, if it is found that the greater part of the profits come from lines of business which the reporting entity has considered to be of high risk, the entity should adopt more exhaustive mitigation measures since its degree of exposure to product- and service-based risk will be higher.

Annex II of this Guide provides some examples of products which, generally speaking, are associated with a higher ML/TF risk, and it lists the products of highest risk for each sector based on the results of the National Risk Assessment.

Lastly, the annex also lists some types of products which, owing to their nature and characteristics, pose a low risk of ML/TF.

Risk factor 3	Geographical risk

In this section the reporting entity should **identify the jurisdictions to which it is exposed either through its own activity** (target markets on which it focuses) **or through the activities of its customers and beneficial owners.**

In this respect, the reporting entity's degree of exposure to the jurisdictions in question will be based on its own activities and the products and services which it offers, and its location or the location of its branches, subsidiaries or local offices. Likewise, the degree of exposure may also be determined by the activity of the reporting entity's customers when (i) the customer is located or operates in the jurisdiction in question; (ii) it is the jurisdiction where the customer obtains financing or it is the source of the funds provided; (iii) it is the jurisdiction where the customer sells the greater part of his products or provides the greater part of his services; (iv) it is the jurisdiction where the customer purchases the greater part of his raw materials necessary for the performance of his activity; or (v) the customer is linked to the jurisdiction through networks, agencies or suppliers or through the destination of the transactions which the customer carries out, among other cases.

Once the jurisdictions to which the reporting entity is exposed have been identified, it is necessary to **assess which risk of laundering of money or assets or terrorist financing is posed by each such jurisdiction**, giving special attention to the jurisdictions which pose a higher risk.

Annex III of this Guide lists some of the factors to be considered when determining which jurisdictions pose a higher risk of ML/TF, and some of the areas which present a potentially lower risk.

Aside from the ML/TF risk of each jurisdiction to which the reporting entity is exposed, consideration should also be given to other aspects, such as for example the degree of political stability of the jurisdiction in question, the level of effectiveness of its legislative and supervisory regime, the level of corruption or the level of financial inclusion.

Additionally, another significant element is the experience of the reporting entity. For example, a reporting entity accustomed to working internationally will not assign the same classification to this risk factor as other reporting entities with limited experience in this field.

Risk factor 4	Transaction-based risk

For this risk factor, the reporting entity should identify all the transactions in which it participates or which it facilitates, and assess the level of the risk that such transactions may be linked to the proceeds of a criminal activity. Consequently, the reporting entity should take into account the volume and size of its transactions, considering its usual

activity and the profile of its customers, as well as the risk associated with the means of payment used.

It should be pointed out that this risk factor is of greater significance in reporting entities which administer customers' accounts, as in the case of banking and non-banking financial entities, since they should identify the types of transactions which are made through those accounts and assess the risks associated with each of these types of transactions.

Annex IV of this Guide lists some high-risk elements associated with transactions, transfers or operations.

Likewise, aside from the risks inherent to any type of transaction, it will also be necessary to take into account the frequency and the number of transactions, especially in the case of the transactions linked to one same customer, and the circumstance of whether they are of complex character, since all these characteristics entail that the transactions are more difficult to monitor and to control.

Risk factor 5	**Distribution channel-based risk**

In this section the reporting entity should consider all the means which are used to interact with its customers and the degree of proximity to its customers. There are distribution channels which may entail a greater risk since they may hinder the identification of the customer and/or beneficial owner. In particular, the reporting entity should take into consideration the extent to which it works with its customers directly and whether it establishes or maintains non-in-person business relations.

Annex V of the Guide lists some of the factors to be considered when assessing this risk.

6. HOW SHOULD THE IDENTIFIED RISKS BE ASSESSED?

In Stage Two the reporting entity should **analyse the risks** that have been identified in each of the categories defined in the previous section. One of the most recommendable ways to analyse the risks is to do so on the basis of a combination of the **probability** of their occurrence and the **impact** of the cost or the losses that would be entailed if the risk in question were to occur.

The **probability** should consider the extent to which it is possible that the reporting entity will be used for the laundering of money or assets or terrorist financing by its customers through the products, services, distribution channels or transactions which the reporting entity provides. Probability may be estimated, for example, on the basis of the number of times a year that it is thought that the risk under analysis may arise. In all cases, the lowest probability levels correspond to improbable or uncommon but in no case impossible situations.

The probability that a risk may occur is calculated by taking into account the **threats** to which the reporting entity is exposed and the **vulnerabilities** of the reporting entity's controls. These two concepts are based on the following:

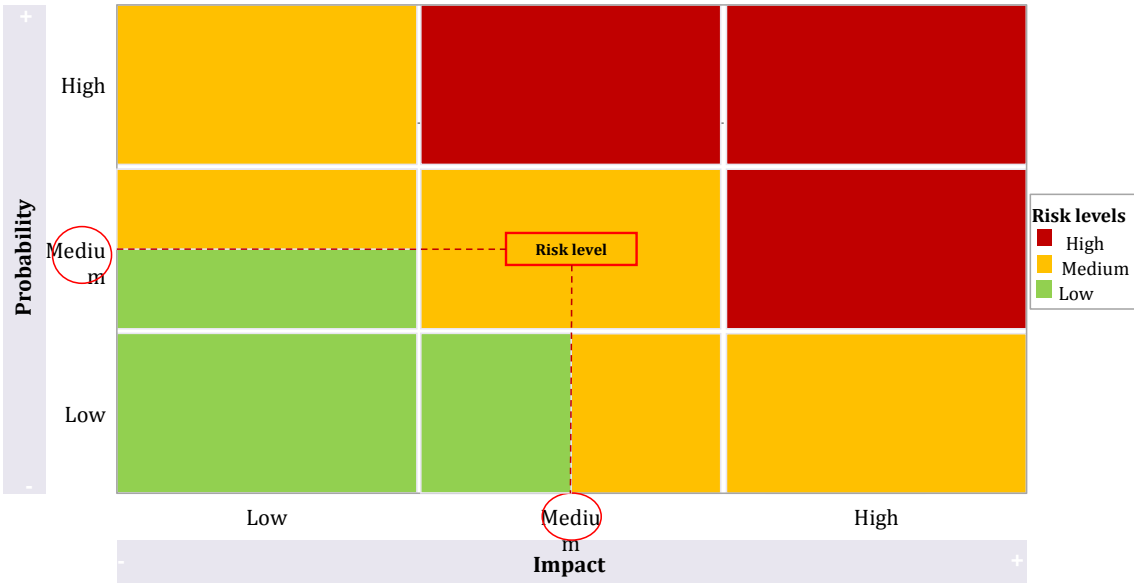
- A *threat* is an external risk factor to which the reporting entity is exposed as a result of the sector to which the entity belongs, of the geographical area in which it is located, or of the economic situation, among other aspects.

- A *vulnerability* is an internal risk factor consisting in shortcomings and deficiencies of the reporting entity's control systems. It also involves the degree of response which the reporting entity is capable of providing. These vulnerabilities may be exploited by external threats.

For its part, the **impact** may be measured as the economic losses or damages which would be produced in the reporting entity's business by the materialization of the risk, either as a result of the crime properly speaking or of the sanctions which the supervisory authorities may impose on it, and as a result of the reputational damage which would be entailed for the reporting entity or even for the whole sector or country in which it operates. In this respect, the impact would be smaller if there were only to be consequences amounting to small sums and/or of short-term effects and the impact would be large or critical if the consequences were to involve large amounts and/or of long-term effects and could affect the normal functioning of the reporting entity.

This estimation of probability and impact should allow a **definition of the ML/TF risk level** (between **High**, **Medium** and **Low**) **for each of the identified risks**, that is to say, for each customer, product, service, jurisdiction, transaction and distribution

channel. This could be represented graphically, by way of example, in the following manner:



Some specific examples of analysis of the associated risk, calculated in terms of probability and impact of some types belonging to one of the risk factors defined in the preceding section, may be found in **Annex VI** of this Guide.

In any case, the analysis of the risk categories and of the combination of probability and impact is **specific to each reporting entity**.

Moreover, all these factors cannot be taken into account only on an isolated basis but rather they should be considered in a **combined way**, that is to say, to give an example, a product classified as being of low risk which is acquired by a customer from a jurisdiction considered to be of high risk may result in an estimation of high risk for that specific combination.

7. WHAT CONCLUSIONS SHOULD THE IRA ALLOW TO BE DRAWN?

Once the risk level of each of the analysed areas has been defined, the reporting entity **should be able to estimate the overall risk level for its business**, which will be the result of the combination of all the various factors and which will differ from one reporting entity to another.

Consequently, a **risk matrix** representing the conclusions of a reporting entity's risk study could be as follows:

		Risk evaluation				
		Probability (+)	*Impact* (=)	*Risk*	*Risk factor*	*Reporting entity risk*
Risk factors	*Customer A / Category A*	Low	High	Medium	**Medium**	**Medium**
	Customer B / Category B	High	Low	Medium		
	Customer C / Category C	Medium	Medium	Medium		
	Product A / Category A	Low	Low	Low	**Medium**	
	Product B / Category B	Low	High	Medium		
	Product C / Category C	Medium	High	High		
	Country A / Category A	Medium	High	Medium	**Medium**	
	Country B / Category B	Low	Medium	Low		
	Country C / Category C	Medium	Low	Medium		
	Operation A / Category A	High	High	High	**High**	
	Operation B / Category B	High	Medium	Medium		
	Operation C / Category C	Medium	High	High		
	Channel A / Category A	Low	Low	Low	**Low**	
	Channel B / Category B	Low	Medium	Low		
	Channel C / Category C	Medium	Low	Low		

It should be kept in mind, however, that the **risk levels** assigned to each of the categories and the overall risk level of the reporting entity **are not static or defined**, but rather these risk levels will change in step with the changes in the reporting entity's circumstances (external threats, size, organizational structure, etc.).

8. WHAT MEASURES SHOULD BE ADOPTED TO DEAL WITH THE RISKS WHICH HAVE BEEN IDENTIFIED AND ASSESSED?

In this stage of the assessment, the reporting entity should **manage** the identified and analysed ML/TF risks. To this end, the reporting entity should **establish some suitable internal control policies and procedures** adapted to the nature, size and characteristics of its business.

These policies, controls and procedures should be addressed to the **mitigation of the identified and analysed risks**, reducing them to a level which the reporting entity considers acceptable (depending on its risk tolerance), in order to avoid or minimize threats, vulnerabilities and impacts, as well as associated reputational, operational or sanctioning risks, among others.

Likewise, the individual risk assessment should allow the identification of the business areas which are most vulnerable to use for ML/TF, whereby the higher the estimation of risk of a specific area, the more control measures should be implemented and the more exhaustively or more frequently they should be reviewed.

In this respect, as control measures, the reporting entity may consider the implementation of control measures that include, without being limited to, the following, which are given here by way of example:

- Establishment of an effective system of application of due diligence measures which is proportional to the identified and analysed risks.

- Definition of scenarios of application of simplified and enhanced due diligence measures, adapted to the nature of each reporting entity, in addition to the measures provided in Law 14/2017 in its Articles 11 and 12, respectively.

- Establishment, by the top management, of an approval system of specific business relations or transactions of greater risk defined by the reporting entity.

- Establishment of limits for the amounts involved in specific transactions considered to be of high risk, such as cash payments.

- Establishment of an effective system of risk categories for the classification of customers, in line with the diligence measures to be applied for each category.

- Determination of a system of periodic reviews of the business relations which are maintained, establishing a higher frequency of review for those relations which are defined as being of higher risk. Verification that the review procedure is carried out by a different person or area of the reporting entity than the person or area

which started the respective business relation, in order to ensure the independence of such procedure.

- Periodic review of the fitness and propriety of the personnel who are in direct contact with the customers, products or areas defined as being of higher risk.

- Provision of training on ML/TF for all personnel, especially (that is to say, more frequently and with more detailed contents adapted to positions) for the personnel who work in the business areas identified as being of higher risk.

- Analysis of the regulatory framework in terms of prevention of ML and the fight against TF of the jurisdictions for which there is a higher degree of exposure either through the reporting entity's activities or through those of its customers.

- In extreme cases, termination of the business relation or discontinuation of a product or service.

9. HOW SHOULD IMPLEMENTED MEASURES BE FOLLOWED UP?

In the last stage of the individual risk assessment, the reporting entity should regularly **review and monitor** the fitness and effectiveness of the mitigation measures which it has implemented as a result of the assessment. That is to say, a continuous follow-up should be carried out in order to verify that the implemented risk management measures are consistent with the identified and analysed risks and to check their degree of effectiveness.

In order to carry out this process of monitoring, follow-up and verification of effectiveness, the reporting entity can take into consideration, among other factors, the following: the results of the internal control policies which it has established; the reports, analyses and verifications which its compliance department has carried out (in the event that the reporting entity possesses such a department); the results of the internal audit (in the case of financial reporting entities); the number of suspicious transactions notified internally to the Internal Control and Communication Body (ICCB) and the suspicious transaction reports submitted to UIFAND; the results of the annual external audit (in the case of financial reporting entities); and/or the recommendations which UIFAND has made in its inspection reports, in the event that the reporting entity has been subject to inspections.

10. OTHER FREQUENTLY ASKED QUESTIONS

Q1. Who should make an Individual Risk Assessment (IRA)?

A1. All reporting entities, as defined in Article 2 of Law 14/2017, should carry out an individual risk assessment. The only possible exception to this are the entities or sectors which UIFAND were to establish and to which it were to so notify expressly as provided in Article 5.3 of Law 14/2017.

On the date of publication of this Guide, UIFAND has not excluded any reporting entity from the obligation to make an IRA.

Q2. Should all the entity's customers/activities be taken into consideration when making an IRA?

A2. No, the IRA should **only** take into consideration the **activities which are subject to the laws in force on prevention of the laundering of money or assets and terrorist financing**, that is to say, the activities which determine its status as a reporting entity as defined in Article 2 of Law 14/2017. Likewise, the assessment should only take into consideration the customers or categories of customers to whom products or services referred to in the aforementioned article have been provided.

Q3. What sources may be consulted for the performance of the assessment?

A3. Aside from the internal considerations and risk factors which have been described in this Guide, the reporting entity may consult other sources when performing its individual risk assessment, including the following, among others:

- Financial reporting entities which have established **internal auditing** procedures may take into consideration the results of such procedures when carrying out the IRA.
- The results of the **National Risk Assessment (NRA)** relating to the sector to which the reporting entity belongs.
- Other **relevant external sources** such as, for example, national risk assessments of other jurisdictions, lists published by intergovernmental organizations or national governments, assessment reports on types of money laundering or terrorist financing published by **FATF** or equivalent bodies such as, for example, **Moneyval.**

Notwithstanding, it should be kept in mind that the aforementioned sources should considered **just one of a series of elements,** supplementing for their part the information contained in the individual risk assessment, but **they should not form the main basis or the totality of the IRA**.

Q4. May the services of an external consultant or adviser be contracted for the performance of the IRA?

A4. Yes, inasmuch as the laws in force do not set any limitation in this respect. Notwithstanding, it should be remembered that the reporting entity has the best knowledge of its own activities and customers and that the entity is the party ultimately responsible for ensuring that the content of the assessment provides a true picture of the reality of its business.

Q5. In what format should the IRA be prepared?

A5. As provided in Article 5.1.a) of Law 14/2017, the individual risk assessment should be **duly documented and recorded in a written report.**

Q6. Who should approve the individual risk assessment?

A6. As provided in Article 3.3 of the Regulation for Application of Law 14/2017, the individual risk assessment should be approved by the **Administration Body** of the reporting entity.

Q7. When is the deadline for the performance of the individual risk assessment?

A7. All reporting entities should have completed their individual risk assessment by **18 July 2019** inasmuch as Law 14/2017 provides, in its Transitory Provision Four, that the time for the completion of the IRA is two years counting from the entry into force of the aforesaid Law (19 July 2017).

Q8. Should the individual risk assessment be submitted to UIFAND?

A8. No. As provided in the laws in force, the assessment should be at the disposal of UIFAND once the legal term for its completion has elapsed. **The IRA should only be submitted to UIFAND in the event that the Unit so expressly requests.**

Q9. What are consequences of not carrying out the individual risk assessment?

A9. The breach of the obligation to carry out the individual risk assessment in the terms established by Law 14/2017 and its Regulation for application **constitutes a very serious offence** according to Article 71.10 of the aforementioned Law. Moreover, the making of **an individual risk assessment which is not fit, proper, objective and realistic will constitute a serious offence unless it is determined that it constitutes a very serious offence** as provided in Article 72.15 of said Law.

It should be recalled that the commission of **very serious offences is punished by:**

1) For legal-entity reporting entities (Article 74.1 of Law 14/2017):

a) Fine from 90,001 to 1,000,000 euros.
b) Temporary or permanent restriction of specific types of transactions.
c) Revocation or modification of the authorization for the respective activity.

2) For natural-person reporting entities (Article 75.1 of Law 14/2017):

a) Fine from 25,001 to 300,000 euros.
b) Minimum temporary suspension of six months or permanent suspension.
c) Temporary or permanent restriction of specific types of transactions.
d) Revocation or modification of the authorization for the respective activity.

For their part, **serious offences are punished by:**

1) For legal-entity reporting entities (Article 74.2 of Law 14/2017):

a) Fine from 15,001 to 90,000 euros
b) Temporary restriction of specific types of transactions.

2) For natural-person reporting entities (Article 75.2 of Law 14/2017):

a) Fine from 3,001 to 25,000 euros.
b) Temporary suspension from one to six months.
c) Temporary restriction of specific types of transactions.

Q10. How often should the IRA be updated?

A10. Once the IRA has been drafted for the first time, in accordance with Article 5.1.c) of Law 14/2017 it should be regularly updated. An updating frequency of every **three years** is recommended with the aim to ensure that the detected ML/TF risk areas will remain current and to take into account the new legislative aspects and new trends and types which arise nationally and internationally in the field of prevention of the laundering of money or assets and terrorist financing.

Likewise, significant **changes** may arise in the variables used in the performance of the IRA which **justify a revision of the IRA sooner than the recommended time** for its periodic revision, such as situational changes or changes in the reporting entity with respect to its business strategy, its organization or structure, or its risk tolerance.

11. ANNEXES

The lists which are included in this section are provided only as examples and are not limiting.

Annex I – Customer risk-based risk scenarios

High risk

It should be recalled that not all the following scenarios are grounds for automatically classifying a customer who presents them as a "high risk customer", but they do mean, in any case, that the reporting entity should give them special attention in order to confirm whether in effect, they do entail a high risk of ML/TF:

- Customers who carry on the business relation or make transactions under unusual circumstances such as, for example, an unjustified geographical distance between the reporting entity and the customers' location or who make, in a frequent and unjustified way, movements of funds between accounts in various jurisdictions.
- National customers who are residents in or have links to some high-risk jurisdiction (see "*Annex III – Risk scenarios relating to geographical risk*").
- Uncooperative customers or those who show an unjustified apprehension with respect to their privacy (refusal or reluctance to provide information requested by the reporting entity).
- Customers whose complex characteristics and structure make it difficult to identify their beneficial owner or the person exercising their effective control.
- Customers who act through third parties such as representatives, attorneys-in-fact, trustees, family members, etc.
- Legal-entity customers which are administered by lawyers, administrative services agents and/or providers of professional services to companies and trusts.
- Customers who are non-profit bodies (associations or foundations), especially including those which operate internationally and, more specifically, in risk jurisdictions.
- Shell or front persons or legal structures without real economic activity or which are personal wealth management vehicles.
- Companies which have nominative shareholders or which are incorporated with bearer shares.
- Customers which carry out their professional activity in high-risk sectors such as:
    - Businesses which involve the use of large amounts of cash and/or the frequent use of cash.
    - Merchants dealing in goods of high value.
    - Casinos and other gambling operators, both in-person and online.

  - Businesses without physical presence which operate only through the Internet.
  - Weapons sector.
  - Company services providers.
  - Intermediaries/commission agents.
  - Any other business with a high international exposure.

- Customers who are politically exposed persons (PEPs), especially including foreign PEPs, and legal entities which, in the end, are controlled by a PEP. This also applies to family members and affinitive persons of a PEP, as provided in Articles 3.7 and 3.8 of Law 14/2017.
- Customers who, in order to prove their professional activity, present service provisioning contracts without specifying the nature of such services or the terms connected with same.
- Governmental, public and parapublic entities, and especially those located in or which are linked to jurisdictions marked by high levels of corruption.
- Customers who are known to have been convicted for offences or against whom a legal procedure has been initiated.
- Customers whose lifestyle or whose transactions are not consistent with the personal and business information which the reporting entity possesses on them.
- Customers about whom there are doubts due to negative news in open sources or in commercial databases.
- Customers who show a high rate of rotation (that is to say, for example, a customer who carries out a commercial activity for a short period of time under one company, which he subsequently closes, going on to operate under a new company).
- Customers who are carrying out a commercial activity which is outside their usual activity or outside the range of products or services which they usually offer.
- Customers who possess great wealth or high purchasing power.
- Customers who possess multiple bank accounts, whether at national level or abroad.
- Customers who have changed advisers a number of times over a short period of time without a justifiable reason for doing so.
- Customers to whom another professional has denied the product or service which they are requesting from the reporting entity with which they seek to establish a business relation or to carry out an occasional transaction.
- Newly-created legal entities for which a small amount of information is available to prove their professional activity.
- Occasional customers.
- Customer portfolios which, generally, have a high rotation or a low level of stability.

Low risk

- Entities listed in the securities exchange which are subject to reporting requirements (either in accordance with the rules of the securities exchange or with a law or other mandatory instruments) which set obligations addressed to ensuring the proper transparency of real title.
- Public companies or administrations.
- Customers who are residents in low-risk geographical areas (see "*Annex III – Risk scenarios relating to geographical risk*").

Annex II – Risk scenarios relating to products and services

High risk

General cases:

- Products and services which have been identified as being of high risk by credible international sources.
- Products which can easily cross international borders.
- Products which inherently favour anonymity.
- Complexes and/or scarcely transparent products.
- New products, innovative products or products which arise from the use of new technologies.
- Products which entail large cash payments.
- Remote non-in-person products or services.
- Products which do not have a market price and which are difficult to value.

By sectors:

	Examples of products and services of higher risk
Bank sector	• International banking correspondent relations. • Private banking activities (at national or international level). • Numbered accounts. • Omnibus accounts. • Specific types of bank accounts which offer greater facilities or advantages such as, for example, lesser restrictions or higher transactional thresholds. • Currency exchange services. • On-line or mobile banking services. • Electronic payment services, such as prepayment cards. • Commercial financing, especially for foreign trade. • International electronic transfers. • Credit activities, particularly loans guaranteed by negotiable instruments or other guarantees. • Safety deposit boxes / safes.
Non-banking financial entities	• Wealth and/or assets management. • Intermediation activities, especially involving complex financial instruments such as structured products, alternative investments, preferred shares, derivatives or collective

	investment funds.
Insurance	• Investment-life insurance policies, especially unit-linked policies (linked to participation in an investment fund).

Economists, auditors, accountants, tax consultants, administrative services bureaus and company services providers	• Trust management services.
	• Provision of company services.
	• Incorporation of companies, especially:
	  ○ Structures administered by lawyers, administrative services agents and/or professional providers of services to companies and trusts.
	  ○ Structures without apparent economic activity.
	• Planning/national and international tax optimization schemes.
	• Accounting services for which there are doubts as to whether the accounts and records on which advice is provided may have been falsified.

Legal sector	• Incorporation of companies, especially:
	  ○ Structures administered by lawyers, administrative services agents and/or professional providers of services to companies and trusts.
	  ○ Structures without apparent economic activity.
	• Legal advice on the purchase and sale of real estate and commercial entities.
	• Management of money, securities and assets, and bank, savings or securities accounts of the customer.
	• International tax consultancy.

Real estate sector	• Purchase and sale of real estate.
Merchants of goods of high value	• Trade with articles of high value, such as vehicles or precious stones and metals, in the cases in which payment is made in cash for a value equal to or greater than 10,000 euros, whether it is carried out in a single transaction or in several operations between which there would appear to be some type of relation.
Postal money order sector	• Services of transfer of money to high-risk jurisdictions (regardless of whether this is done by remittances or through postal current accounts).
Gambling casinos (in-person or online)	• Collection of prizes and/or making of bets for a value equal to or greater than 2,000 euros, regardless of whether such bets are made in a single transaction or in several operations between which there would appear to be some type of relation.

Low risk

- Life insurance with a low annual premium or single premium[1].
- Insurance policies for pension plans, as long as they do not contain an early redemption clause and cannot be used as a guarantee.
- Pension, retirement and similar plans which provide for the payment of retirement benefits to employees, as long as the contributions are made by deductions from wages and the rules of the plan do not allow beneficiaries to assign their participation.
- Properly defined and limited financial products or services addressed to specific types of customers for the purpose of financial inclusion, such as consumer loans or savings products.
- Products for which the risk of the laundering of money or assets or terrorist financing is managed by means of other factors such as, for example, limits on the withdrawal of cash or ownership transparency.

[1] More specifically, Law 14/2017, in its Article 11.2.a) establishes *life insurance policies with an annual premium that does not exceed 1,000 euros or with a single premium that does not exceed 2,500 euros* as one of the hypotheses in which simplified due diligence measures may be applied.

Annex III – Risk scenarios relating to geographical risk

High risk

- Jurisdictions with deficiencies in their controls of the fight against the laundering of money or assets or terrorist financing which are listed by international bodies like the Financial Action Task Force (FATF), the European Union (whose listings are communicated by UIFAND through the respective Technical Communiqués), the International Monetary Fund or the World Bank.
- Jurisdictions which, according to reliable sources, such as mutual assessment or follow-up reports of FATF or of equivalent bodies such as Moneyval, do not possess effective systems to fight the laundering of money or assets and terrorist financing.
- Jurisdictions subject to sanctions, embargoes or other similar restrictive measures applied by such bodies as the United Nations or the European Community.
- Jurisdictions identified by credible sources as having high levels of corruption, organized crime or any other criminal activity.
- Jurisdictions which, according to credible sources, finance or support terrorist activities.
- Offshore financial centres.

Low risk

- Member states of the European Union.
- Countries which, according to credible sources, have a low level of corruption or of other criminal activities.
- Countries which, according to credible sources such as, for example, mutual assessment or follow-up reports of FATF or of equivalent bodies such as Moneyval, possess an effective system for the prevention of and fight against the laundering of money or assets and terrorist financing as per FATF recommendations.

Annex IV – High risk scenarios relating to transaction-based risk

- Transactions of sporadic or isolated character.
- Payments received from unknown parties or from third parties not associated with the customer.
- Transactions involving excessively large amounts or amounts which are larger than necessary to formalize the transaction concerned.
- Transactions for amounts below or above the market price.
- Payments in cash or in other similar instruments of high liquidity.
- Transfer between accounts of one same customer or between digital accounts, wallets or purses.
- Regular transactions whose beneficiary is the same individual (whether a natural person or a legal entity) or same group of individuals.
- Transactions which do not apparently make economic or commercial sense or which are not consistent with the knowledge of the customer, his expected behaviour or his economic possibilities (level of wealth, savings capacity...).
- Transactions which the customer requests and which do not lie within the area of experience of the reporting entity or are not among the products or services which the entity customarily provides.
- Transactions in which the funds are of personal origin or in which the funds are not of an easily identifiable origin.
- Transactions in which the funds come from abroad, especially if the jurisdiction in question does not appear to bear any relation to the customer or to his operations.
- Transactions (such as international electronic transfers) whose destination is high risk countries (such as offshore jurisdictions).
- Transactions in which it is suspected that the beneficiary may be a financial vehicle corporation or a shell company.
- Sleeping bank accounts which suddenly become active again for no apparent reason.
- "Bridge" accounts.

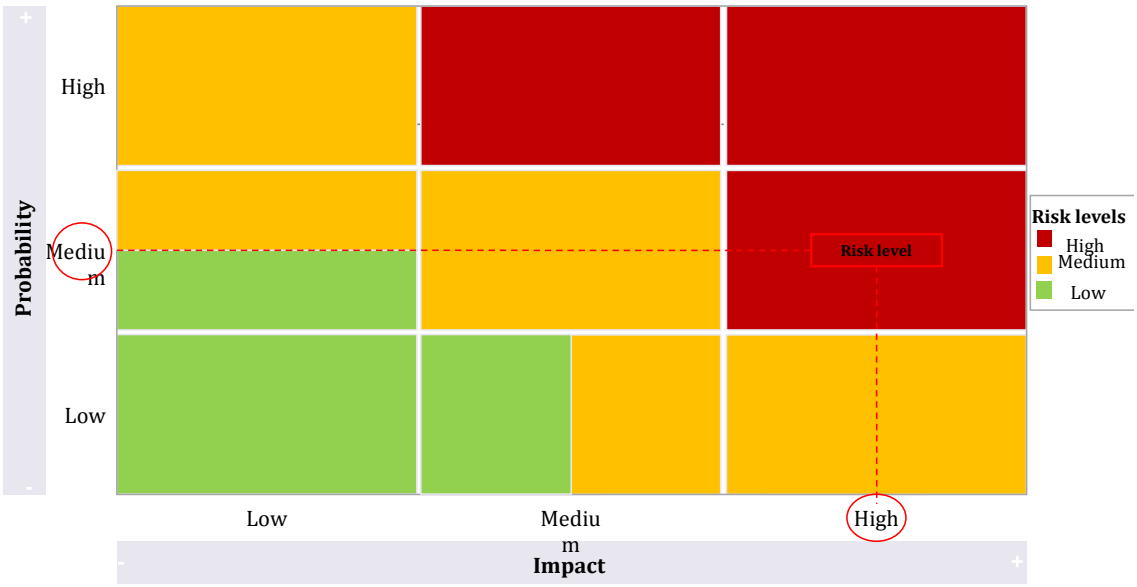
Annex V – High risk scenarios relating to distribution channel-based risk

- Non-in-person (online) distribution channels.
- Distribution channels which use technology (especially new technologies) for the establishment and/or maintenance of business relations with customers.
- Use of advisers, intermediaries and agents, especially in the cases in which work is carried out with the customer solely through such intermediaries.
- A high dependence on third parties for the practice of due diligence measures. In such cases, this dependence and the quality of the information obtained through such third parties to supplement the reporting entity's own due diligence measures should be justified.[2]

[2] It is recalled here that delegation of due diligence measures to third parties should comply with the requirements provided by Article 18 of Law 14/2017. In this respect, the Law only allows the delegation of the identification and verification of the identity of the customer and of the beneficial owner, as well as the procurement of information on the purpose and nature of the business relation, but not the application of continuous follow-up measures. In all cases, the delegating reporting entity continues to be responsible for the fulfilment of these obligations.

Annex VI – Examples of risk estimations based on probability and impact levels

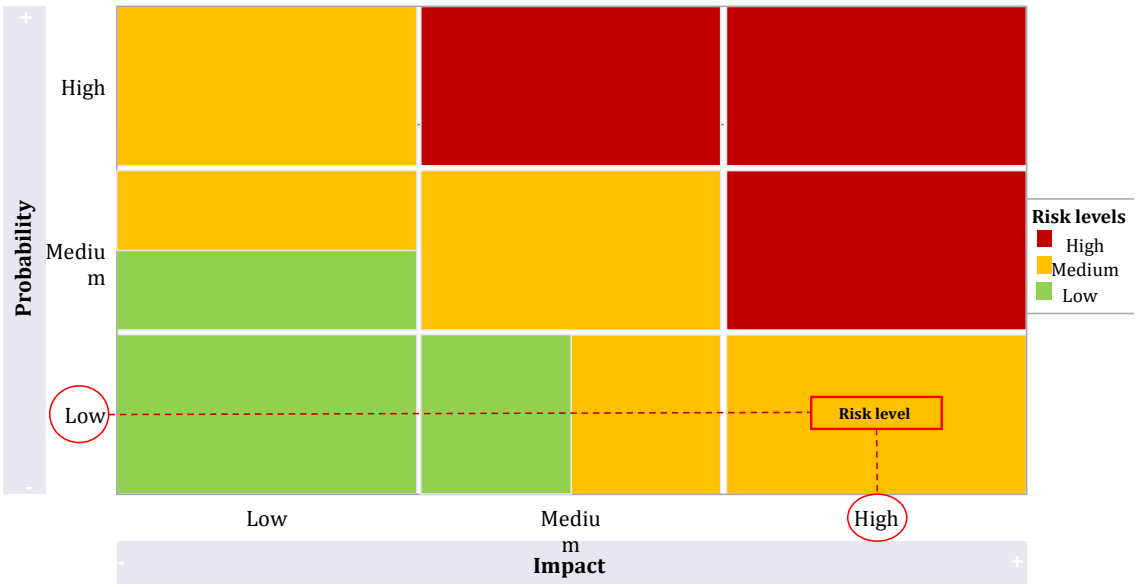
Example 1 – Risk according to type of customer: small companies



This ML/TF risk classification relating to small companies **could correspond** to that of a reporting entity in which the majority of its customers are of this type and operate locally, are exposed to cash payments, have a simple control structure, and may have representatives and attorneys-in-fact who act on their behalf.

In a case such as this, the reporting entity could consider that the probability that the source of the funds which this type of customers provides may be illegitimate is not particularly high and for this reason the entity gives the probability risk a **"Medium"** classification. Notwithstanding, bearing in mind that most of its portfolio of customers would be formed by this type of companies and that the economic and reputational impact would be quite substantial, the impact risk would be classified as **"High"**. Consequently, the reporting entity could consider that the overall ML/TF risk level entailed by this type of customers for the entity's business is **"High"**.

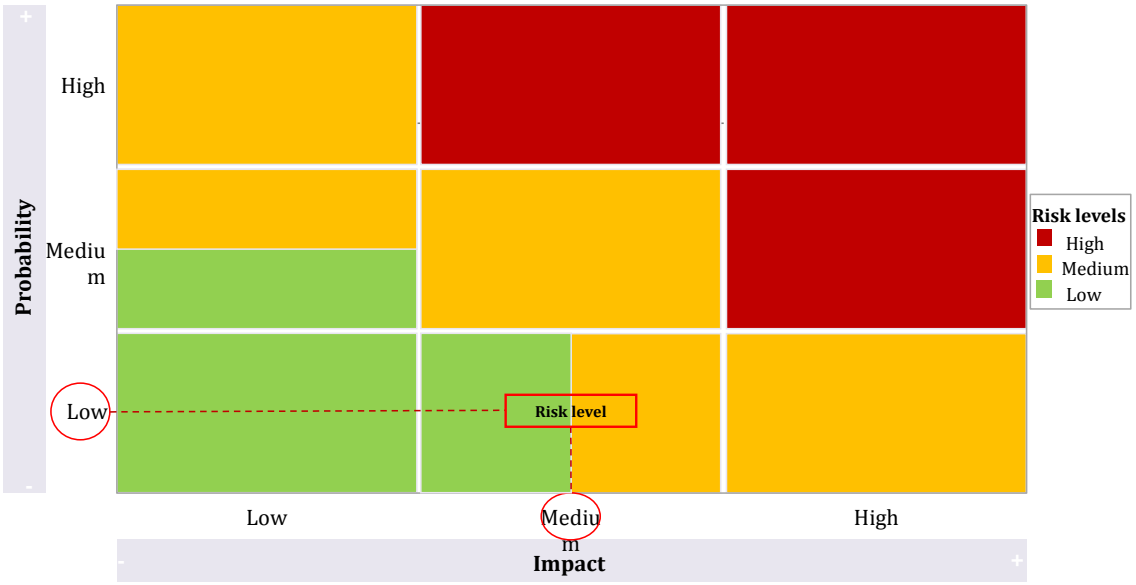
Example 2 – Risk according to type of customer: multinationals



This classification of the ML/TF risk associated with multinationals **could correspond** to that of a reporting entity which has a single multinational company in its customer portfolio but such multinational customarily operates abroad, its beneficial owner is a foreign national and it has a complex shareholding and control structure.

In a case such as this, the reporting entity could consider that the probability that this type of customers could use it for ML/TF purposes is **"Low"**, inasmuch as only a single customer in the entity's portfolio represents a very small percentage of the portfolio. Notwithstanding, in the case in which this risk were to materialize, the impact would be **"High"**. Consequently, the reporting entity could consider that the overall ML/TF risk entailed by this type of customers for the entity's business is **"Medium"**.

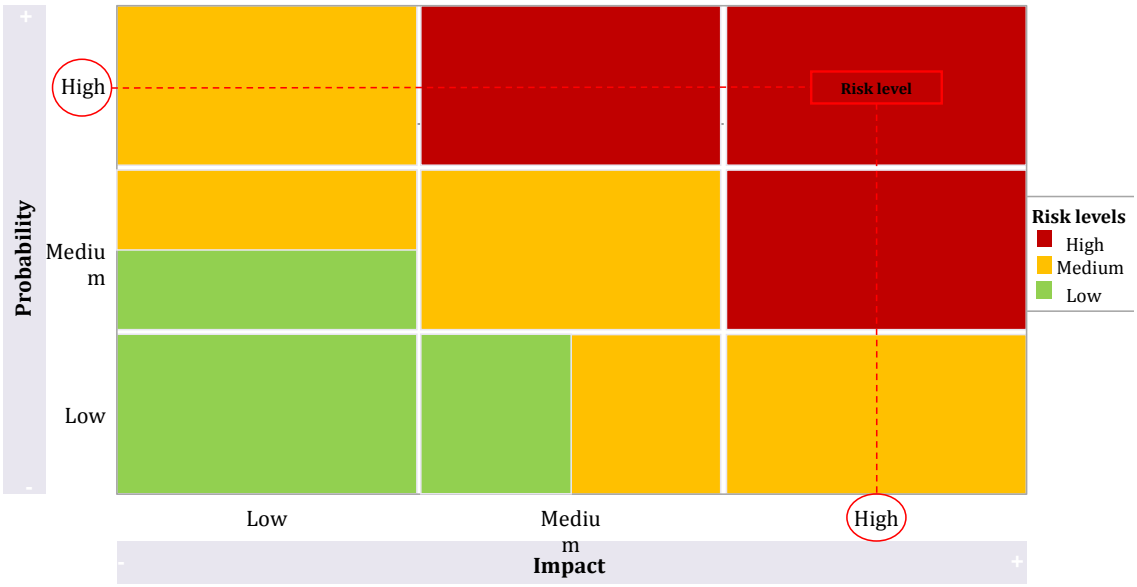
Example 3 – Risk according to type of product: life insurance policies



This classification of ML/TF risk associated with life insurance policies **could correspond** to that of a reporting entity which commercializes low-complexity life insurance products, in which the premiums are usually of small amounts paid through bank accounts, and the redemption of the premiums is not allowed. Moreover, the entity only commercializes the products to residents and nationals.

In a case such as this, the reporting entity could consider that the probability of this product being used for ML/TF purposes is **"Low"** and that, in turn, the impact risk for the entity's business would be **"Medium"** since the greater part of the products of its portfolio are life insurance policies. Consequently, the reporting entity could consider that the overall ML/TF risk for this type of product with respect to the entity's business is **"Low"**.

Example 4 – Risk according to type of product: prepayment cards



This classification of ML/TF risk associated with prepayment cards **could correspond** to that of a reporting entity which is just beginning to offer a new service and which does not yet have a very clear idea about its use. Moreover, the funds for this type of product are usually charged by means of cash deposits.

In a case such as this, the reporting entity could consider that the probability of this product being used for ML/TF purposes is **"High"** and that, in turn, the impact which would be entailed for the entity's business would also be **"High"**, considering that this is a new type of product in which the use of cash is involved. Consequently, the reporting entity could consider that the ML/TF risk level which this type of product entails for the entity's business is **"High"**.