Funded
by the European Union

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Project against Money Laundering and Terrorist Financing in Serbia

MOLI Serbia

DGI(2013) 1 October 2013

TECHNICAL PAPER:
Guidance on risk-based supervision and risk assessments
Prepared by Council of Europe Expert Ms Maud Bokkerink

ECCU-MOLI SERBIA-TP20-2013

September 2013

Table of Contents

GUIDANCE DOCUMENT FOR RISK-BASED AML/CFT SUPERVISION AND FOR ML/TF RISK ASSESSMENT BY FINANCIAL INSTITUTIONS AND DNFBPS

1. Introduction

Recommendation 1 of the 2012 Financial Action Task Force (FATF) 40 Recommendations and its Interpretive Note require supervisors, financial institutions or designated non-financial businesses and professions (DNFBPs) to apply some of the FATF Recommendations in a risk-based manner. In order to apply a risk-based manner to the anti-money laundering and combatting the financing of terrorism (AML/CFT) requirements, supervisors and supervised entities should first understand the money laundering and terrorism financing (ML/TF) risks in their country and of their sectors and business by identifying and assessing possible risks. A risk assessment is a first step a supervisor and a supervised entity should take before developing AML/CFT control measures to ensure that these measures will be appropriate to the nature and size of the business.

The objective of this document is to provide guidance for supervisors and supervised entities on how to perform an overall ML/TF risk assessment with respect to their supervisory process and business operations and which factors can be taken into account.

This document exists of two parts: 1) a description for supervisors on how to develop methods to assist in adopting a risk-based approach to supervision, and 2) guidance for financial institutions and DNFBPs in making a risk assessment of the business and developing a risk management system. This document is intended to be a practical guide on the process of setting up a risk-based approach. For more high level principles on the risk-based approach reference is made to several FATF guidance documents on the risk-based approach.

2. A risk-based approach to AML/CFT inspections

In order to apply a risk-based manner to AML/CFT supervision, supervisors should first understand the ML/TF risks present in their country by identifying possible risks and by assessing their potential impact on the supervised entities.

A risk analysis of potential ML/TF risks is the basis for strategic planning and policy setting. A risk analysis can be done at a strategic level to determine if there are new products or markets that pose an ML/TF risk, at the tactical level to assess the ML/TF risks per sector or type of entities, and at the operational level to assess the risks per entity or group of entities. By determining in advance where the ML/TF risks are high, the supervisor can allocate its resources and define the scope and depth of inspections.

The FATF Methodology for assessing technical compliance with the FATF Recommendations and the Effectiveness of AML/CFT systems states in criterion 26.5 with respect to supervision of financial institutions that the frequency and intensity of onsite and offsite AML/CFT supervision of financial institutions or groups should be determined on the basis of:
(a) the ML/TF risks and the policies, internal controls and procedures associated with the institution or group, as identified by the supervisor's assessment of the institution's or group's risk profile;
(b) the ML/TF risks present in the country; and
(c) the characteristics of the financial institutions or groups, in particular the diversity and number of financial institutions and the degree of discretion allowed to them under the risk-based approach.

Similar for the supervision of DNFBPs, the Methodology states in criterion 28.5 that it should be performed on a risk-sensitive basis, including:
(a) determining the frequency and intensity of AML/CFT supervision of DNFBPs on the basis of their understanding of the ML/TF risks, taking into consideration the characteristics of the DNFBPs, in particular their diversity and number; and
(b) taking into account the ML/TF risk profile of those DNFBPs, and the degree of discretion allowed to them under the risk-based approach, when assessing the adequacy of the AML/CFT internal controls, policies and procedures of DNFBPs.

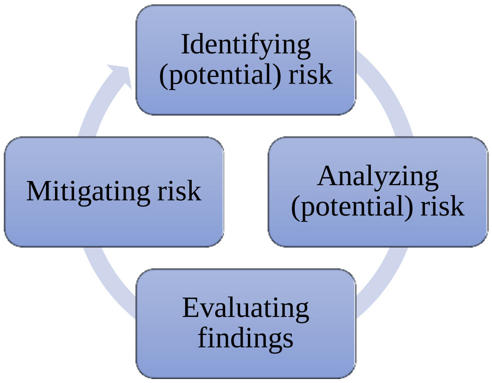
This paper describes several methods that will assist a supervisor in adopting a risk-based approach to supervision:

1. **Assessing the overall ML/TF risk per (sub)sector**[1] to identify (sub)sectors with higher ML/TF risks.
2. **Developing a risk profile per supervised entity** (or group of similar entities) to determine the frequency and intensity of onsite and offsite AML/CFT supervision.
3. **Trend analysis of new ML/TF risks** to ensure that risks are identified early on and can be addressed with mitigating programs.

[1] A subsector is for instance corporate banking within the banking sector; reinsurance within the insurance sector; casinos within the gaming sector.

4. **Thematic approach to AML/CFT supervision** to focus on risk areas and to allow for effective use of sparse supervisory resources.
5. **Risk-based approach to inspections of individual entities** to examine specific issues in depth.

Essentially, the risk-based approach to AML/CFT supervision and the methods detailed below all revolve around the process of identifying, analyzing, evaluating and mitigating ML/TF risks. Additionally, all supervisory authorities should make use of communication to influence the behavior of the entities. Also, FIUs should provide supervisors with statistical information on suspicious transaction reports that can assist in applying a risk-based approach to AML/CFT supervision (e.g., number of reports per reporting entity, sort of transactions reported, time between transaction date and reporting date).



1. **Assessing overall ML/TF risks per (sub)sector**

By assessing the ML/TF risks per (sub)sector, the supervisory authorities can focus their efforts and resources on those (sub)sectors where ML/TF vulnerabilities are higher so that they can have more impact at the tactical level. This does not mean that (sub)sectors with lower risk can be ignored, but supervisory efforts for those sectors can have a lower intensity.

Once the supervisor has determined the risk level of each (sub)sector, the supervisory methods can be determined in line with the perceived risk. As risk increases, so does the complexity of the supervisory toolset. For instance, mainly offsite supervision for lower risk sectors, and for higher risk sectors more onsite examinations.

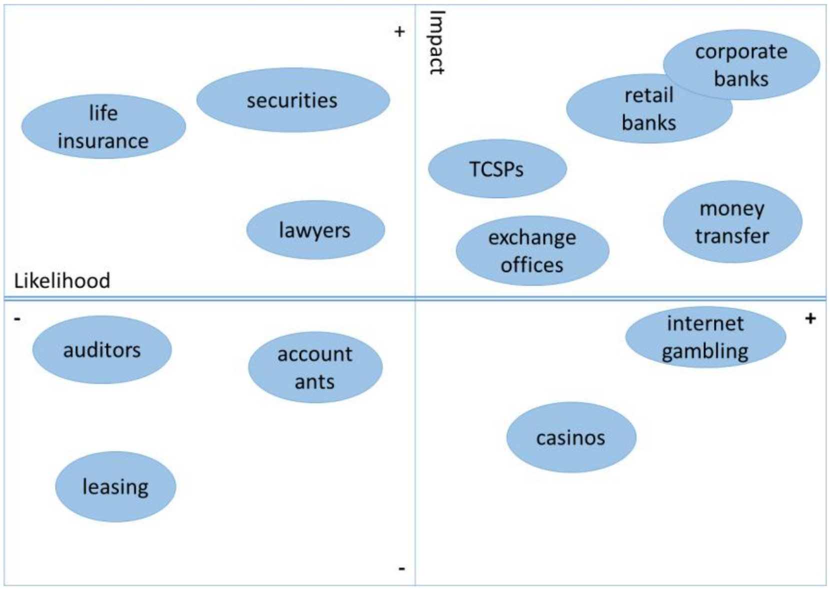
Supervisors can adopt the following methodology when assessing the overall sectoral risk. First, the supervisor will have to assess the likelihood (threats and vulnerabilities) that ML or TF can occur in a (sub)sector. Per sector the supervisor can rate several (inherent) risk factors: cash intensity of the sector, unknown/unclear sources of funds, manner of client contact, entities with operations in high risk countries, client base (e.g., non-resident, high net worth clients, or corporate clients with complex structures), and amount of international business. Additionally, also more objective factors can be used, such as size of the sector, turnover, number of entities. This rating does not take into account the control measures that individual entities have in place. The supervisors can rate the factors in the following way:

Risk factors	Higher likelihood	Lower likelihood
Size of sector	Numerous entities Many entities with operations in high-risk countries	Few or small (in size) entities Entities operate only domestically
Products & services	High number of cash products or cash transactions Complex products Source of funds not always known	Limited/no cash products or cash transactions Simple products Source of funds is clear
Transactions	High value transactions Large number of transaction with persons in high-risk countries	Low value transactions Only domestic transactions
Customers	Many non-resident or high net worth clients Many clients with complex structures	Only domestic clients
Delivery channels	Client contact is never face-to-face	Always direct client contact

Second, the supervisor will have to rate the impact if in a (sub)sector ML or TF indeed occurs. There are different 'levels' of impact that have to be considered: the financial-economic and reputational impact on an entity, on the sector, on the supervisor, and on the country. This rating will be subjective as it is difficult to quantify this impact.

A risk assessment of several (sub)sectors that are obliged under the AML/CFT Law could result in a matrix as below. The matrix below is an example for several sectors. Such a matrix can be developed by all AML/CFT supervisors in a country, but a supervisor should at least make such a matrix for those sectors under its remit. Once such a matrix is developed, a supervisor can determine at a tactical level which sectors need more intense or frequent attention, which supervisory methods can be used to mitigate the risks and which resources need to be allocated.

Besides supervisory methods as onsite and offsite supervision, supervisors can also use communication as a tool to influence behavior of entities. By using the matrix, the supervisor can tailor its communication efforts, for instance by having a seminars for lower risk sectors, but direct or roundtable discussions for higher risk sectors. Also, by means of newsletters, communiqués or cooperation with the sector associations supervisory efforts can be tailored.



Needless to say that the sectors in the upper right quadrant will need more intense and frequent supervisory efforts, such as onsite visits, awareness raising and cooperation with associations. The sectors in the lower right quadrant where the likelihood is higher but the impact low, can for instance be supervised with less intensity or in a lower frequency. The sectors in the upper left quadrant where the likelihood is low but the impact high should ML/TF occur, can be supervised through offsite methods and awareness can be raised through seminars. The sectors in the lower left quadrant can be supervised in a very light touch -offsite- manner.

An assessment of the ML/TF risks per (sub)sector should be reviewed and where necessary revised periodically.

2. Risk profiles of supervised entities

The Interpretive Note to FATF Recommendation 26 states that supervisors should have access to all relevant information on the specific domestic and international risks associated with customers, products and services of the supervised entities. The frequency and intensity of AML/CFT supervision of financial institutions should be based on the ML/TF risks, and the policies, internal controls and procedures associated with the institution, as identified by the supervisor's assessment of the institution's risk profile, and on the ML/TF risks present in the country. Interpretive Note to Recommendation 28 similarly requires supervisors to take into account the ML/TF risk profile of DNFBPs when assessing AML/CFT compliance of DNFBPs.

Supervisors should understand the risk present in a supervised entity. Based on this, supervisors should establish a risk profile of the entities under their supervision based on a risk rating methodology. For larger entities, a supervisor should make an individual risk profile. For smaller entities that are similar, supervisors can make a risk profile that applies to a group of similar entities.

To establish a risk profile of an entity, a supervisor should take account of the nature and extent of the risks associated with countries, customers, transactions, products and services. A supervisor can obtain information on these factors directly from the supervised entities, for instance through questionnaires, or from their ML/TF risk assessments, or from other sources, including the supervisor's information from inspections.

On the basis of a risk profile of an entity, a supervisor can determine the intensity, frequency and scope of offsite and onsite inspections. The supervisor should review the assessment of the ML/TF risk profile of an entity (including the risks of non-compliance) periodically, and when there are major events or developments in the management and operations of the entity.

The actual processes used to determine a risk profile can vary: more formal techniques such as statistical analysis or calculations can be used, but one can also rely on the conclusions of a group discussion or workshop to develop risk profiles. Supervisors should be aware that assessing ML/TF risks requires judgment and is not an exact science.

Countries

Supervisors should develop a list of high-risk countries. At a minimum, this list should take account of the countries identified by the FATF as high-risk and non-cooperative countries or jurisdictions and the countries against which the UN, the EU or other regional or international organisations have imposed sanctions or restrictive measures. Also other relevant risk classifications of countries can be taken into account.

The supervisor can collect information on where the supervised entities undertake their activities. Activities can be daughters, branches, but also major participations or joint ventures. The more high-risk countries where an entity has activities, the higher the ML/TF risks that an entity is potentially exposed to. For a practical approach, a supervisor can decide that an entity that only has domestic activities runs low risk, an entity that is active in 1-5 high-risk countries runs medium risk, and entity that is active in more than 5 high-risk countries has a high exposure to ML/TF risks.

Customers

A supervisor will also need to assess the customer-base of an entity. Depending on the number and types of customers that an entity serves, the inherent ML/FT risk will differ. Certain types of customers can increase the ML/TF risk, especially when there are large numbers of these customers. Examples are large corporations that do international business, corporations with complex structures, private banking customers, non-resident customers, or customers from high-risk countries. On the other hand, when the customer-base consists mainly of domestic retail customers or small enterprises, the risk can be lower.

Transactions, products and services

The types of products that an entity offers can be numerous and diverse. For instance, there will be banks in a country that offer the full range of products and banks that only offer internet savings accounts. Certain products have a higher risk of being used for ML/TF, such as cash intensive products and services, international transactions, and products that facilitate (near) anonymous transactions. Also, the ML/TF risks of entities that mainly have non face-to-face delivery channels will be assessed differently from entities that always have direct customer contact.

Level of compliance

In the risk profile of an entity, the supervisor can also take into account the level of compliance (insofar known). That is the extent to which policies, internal controls and procedures are adequate and implemented. Also, the risk appetite of the entity, the tone at the top, and the awareness of staff can be factored into this.

EXAMPLE ONLY

Factors Entity	Countries	Customers	Product/Services	Level of compliance	Risk profile
Bank A	Activities in more than 5 high risk countries	Non-resident customers, incl. corporations with complex structures	Full range of banking products	On last inspection only minor shortcomings	Medium
Insurer B	Only domestic activities	Domestic retail customers and small businesses	Basic, small premium life insurance No investment products	No policies and procedures; Lack of awareness	Medium
TCSP C	Activities in more than 5 high risk countries	International customers, several PEPs as beneficial owners Several customers with consultancy services	All TCSP-services provided	Policies and procedures present; Lack of awareness on suspicious activities	High

3. Trend analysis - identifying new ML/TF risks

Identifying new ML/TF risks will allow supervisors to determine strategic priorities. A supervisor should continuously undertake this process to identify new risks and trends to ensure that they are detected early on and can adequately be addressed with risk mitigating programs.

Supervisors have to use several sources to see if there are (new) threats of money laundering or terrorism financing. The sources are numerous: there is no comprehensive list of potential information sources and the number of potential threats is practically countless. By checking open sources (internet, twitter, Linked-in groups) supervisors can be alerted to new financial providers, markets, products, payment methods, or ML/TF techniques. Sources can also be counterparts such as other (foreign) supervisors or the FIU. FATF or FSRB typology reports, but also research reports from professional parties or academia can give new insights into ML/TF trends. As trend analysis calls for permanent information gathering, research and analysis, the supervisor should allocate sufficient resources to this.

Based on different signals and information the supervisor should analyse potential threats for the financial and non-financial sectors. The supervisors can consider whether entities indeed provide that product or payment method in the jurisdiction. And if so, the supervisor can then assess the characteristics of the (new) product or payment method, the number and type of clients the product or payment method are offered to, and the amounts involved. Information from domestic and international counterparts, such as the FIU, law enforcement and other supervisors can assist and support the analysis.

Similar as with the overall sectoral risk assessment described under 1, for this trend analysis the supervisor can also evaluate the likelihood that the threat will occur in the jurisdiction and what the impact will be. For instance, it might be less urgent to take immediate action if the problem is only relevant for one entity compared to when it is a common issue for several entities.

4. Thematic approach to supervision

Thematic supervision means that the supervisor will select a risk area and for that risk area will examine a group of entities at an operational level. Certain risks will occur at several entities. Supervision will therefore have to focus on these risk areas in a supra-institutional way. The risk areas can be selected based on the trend analysis described under 3 or based on the results of previous examinations (e.g., entities where similar deficiencies in control measures have been found). Especially when a large number of entities have to be inspected, a thematic approach can be an optimal way for a supervisor to make use of limited supervisory resources.

Once the supervisor has selected a theme, a representative sample of entities has to be selected. This will be entities with similar characteristics and where the risk is likely to be high(er). The sample should include entities with good practices, systems and risk controls which may stand as an example for the peer group and also entities with lesser controls. For instance, if the theme is “clients connected to high risk and non-cooperative jurisdictions”, entities can be selected with activities or clients in those jurisdictions. If the theme is “real estate”, focus has to be on entities that have real estate investments or serve real estate developers. Or, for the supervisors of money transfer operators a risk-based approach can be that those agents will be inspected that have larger than average remitted amounts (thus, for instance if the average remitted amount is 500 euro, agents with a large number of remitted amounts above 2000 euro, can pose higher risk).

The thematic approach can thus be used for risk mitigation purposes. For this purpose supervision can consist of offsite examinations and/or onsite inspections whereby questionnaires, interviews with staff of the entity and sampling the customer files and transactions will focus on the selected theme.

By examining a number of entities with respect to a certain theme, it will be easier for supervisors to benchmark compliance and to identify outliers within the entities and best practices. The supervisor can publish the generic findings and the best practices and it that way influence the behavior of a sector in a preventive manner.

The thematic approach can also be used for further risk analysis. For this, the thematic approach can for instance exist of offsite information collection of a selected group of entities and review of other (open) sources to further analyse the risk to determine if the risk is relevant for the jurisdiction. The supervisor can thus quickly address new developments within the area of AML/CFT.

5. Risk-based approach to inspections of individual entities

For the inspection of an individual entity a risk-based approach can also be adopted. This can be scheduled regular inspections or special inspections as a result of incidents, complaints or other signals that there are compliance issues (for instance a betting shop that has many winning tickets, or a bank that could have correspondent relationships with banks on UN, EU or other regional or national sanctions lists). The inspection will then focus on the issues concerning that incident or signal.

The scope and depth of the inspection will be determined on the basis of an assessment of the specific issue or the entity's risk profile. By focusing on policies and procedures around the specific issue and discussing implementation of policies and procedures with staff that deal with that issue and sampling only transactions and customer files around that issue, the supervisor can focus on the core problem.

Because of this in-depth inspection, supervision will shift from mainly assessing the existence of policies and procedures to also determining the effectiveness and implementation of the policies and procedures.

RISK ASSESSMENT GUIDANCE FOR FINANCIAL INSTITUTIONS AND DNFBPS

1. Introduction

FATF Recommendation 1 and its Interpretative Note (paragraph 8) require a financial institution or DNFBP to conduct a business related risk assessment of its ML/TF risks. To execute an ML/TF risk assessment, an entity should take appropriate steps to identify and assess the ML/TF risks related to customers, countries or geographic areas, products, services, transactions and delivery channels. A risk assessment enables the entity to focus its AML/CFT efforts and to adopt appropriate measures to optimally allocate the available resources. The entity should document those assessments in writing and keep these assessments up to date. The nature and extent of the ML/TF risk assessment should be appropriate to the nature and size of the business. An entity should always understand its ML/TF risks, but the supervisor may determine that individual documented risk assessments are not required, if the specific risks inherent to the sector are clearly identified and understood.

Based on the risk assessment an entity should have policies, controls and procedures that enable it to manage and mitigate effectively the risks that have been identified. The term 'mitigate' in this context means reducing the seriousness or extent of ML/TF risks. It should monitor the implementation of those controls and enhance them, if necessary. When assessing risk, an entity should consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level of mitigation to be applied. An entity may differentiate the extent of measures, depending on the type and level of risk for the various risk factors.

The risk assessment should be done for each group or type of customers, business relationships, product or services offered by the entity within its business.

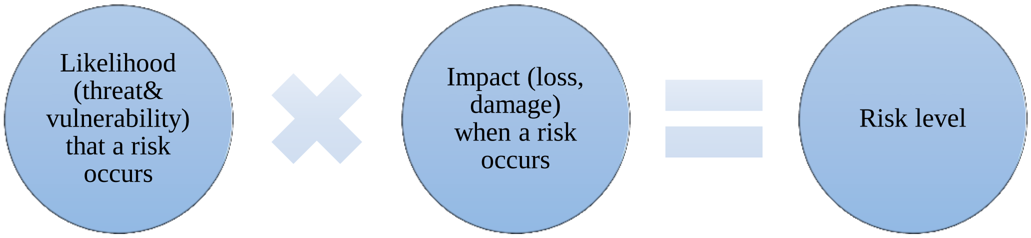
Each entity, regardless of its size and complexity, is expected to develop an adequate risk management system for money laundering and terrorism financing. This risk management system is to ensure that the ML/TF risks should be continuously and comprehensively identified, assessed, monitored, managed and mitigated.

An adequate system of ML/TF risk management should include:

- A risk assessment of money laundering and terrorism financing risks of the business;
- Policies and procedures to control money laundering and terrorism financing risks;
- An organisational structure to execute these risk management controls; and
- A process to systematically check and assess the adequacy of the control systems.

2. Risk assessment of the business

Risk is a function of the likelihood of occurrence of risk events and the impact of risk events. The likelihood of occurrence is a combination of threat and vulnerability, or in other words, risk events occur when a threat exploits vulnerability. Accordingly, the level of risk can be mitigated by reducing the size of the threats, vulnerabilities, or their impact.


Likelihood (threat& vulnerability) that a risk occurs
Impact (loss, damage) when a risk occurs
Risk level

In order to establish the entity's exposure to ML/TF and the efficient management of that risk, the entity needs to identify every segment of its business operations where a ML/TF threat may emerge and to assess its vulnerability to that threat. It is necessary that ML/TF risks are continuously identified at all management levels - from the operational level to the Executive Board - , and to include all organisational units of the entity. The size and complexity of a business plays an important role in how attractive or susceptible it is for ML/TF. For example, a large organisation is less likely to know a customer personally who thereby can be more anonymous than a customer of a small organisation. And an organisation that provides international services might be more attractive to a money launderer than a domestic organisation.

Upon identifying the risks, the entity needs to adequately assess the ML/TF risk exposure, which would enable it to evaluate the likelihood of adverse effects arising from that risk and the potential impact of that risk on the realisation of business objectives.

The risk identification and analysis needs to be conducted for all existing and new products, activities and processes. An effective process of ML/TF risk identification and analysis serves as a basis for establishing an adequate system of risk management and control, and, consequently, for reaching the ultimate goal – minimising possible adverse effects arising from that risk.

An assessment of money laundering and terrorism financing risks proceeds from the assumption that different products and services offered by entities in their business operations, or different transactions executed by them, are not equally vulnerable to misuse by criminals. The purpose of a risk assessment is to apply control measures proportionate to the identified risk. This allows entities to focus on the customers, countries, products, services, transactions and delivery channels that constitute the greatest potential risk.

The process of an ML/TF risk assessment has four stages:

1) identifying the areas of the business operations susceptible to ML/TF;
2) conducting an analysis in order to assess the likelihood and impact of ML/TF;

3) managing the risks; and
4) monitoring and reviewing the risks.

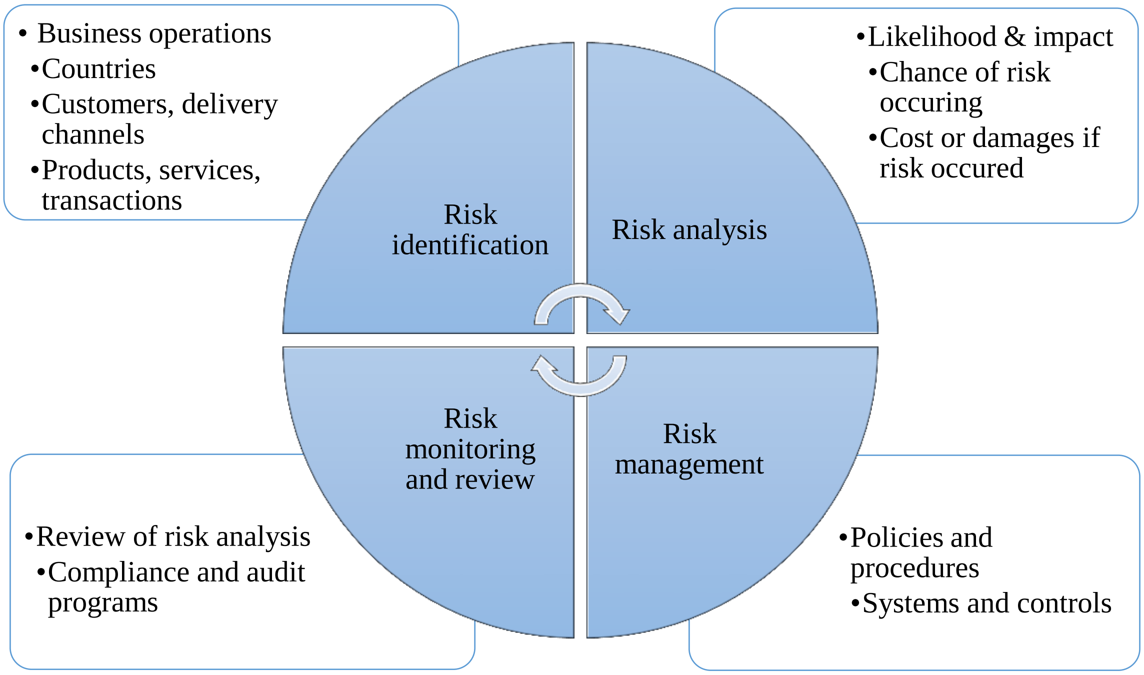
The first stage of the risk assessment is to identify customers, products, services, transactions, and geographical locations specific for the entity. Depending on specific characteristics of and delivery channels for certain customers, products, services and transactions, the threat of and vulnerability to money laundering and terrorism financing varies.

In the second stage, the ML/TF risks that can be encountered in an entity need to be analysed as a combination of likelihood that the risks will occur and the impact of cost or damages if the risks occur. This impact can consist of financial loss to the business from the crime, from fines from the authorities or from enhanced mitigation measures. It can also consist of reputational damages to the business or to the whole sector. The analysis of certain risk categories and their combinations is specific for each entity, so that the conclusion on the total risk level must be based on all relevant information.

In the third stage, the entity will, based on the analysis, apply risk management strategies and implement policies and procedures accordingly. To effectively mitigate the risk, adequate systems and controls will be implemented.

Finally, in this process the risks and the management of the risks have to be monitored and reviewed. An entity can do this by developing a monitoring regime through its compliance and audit programs. The assessment of ML/TF risks must be revised periodically, based on the extent risks have changed or the entities operations or strategies have changed.

RISK ASSESSMENT METHOD



In view of the fact that the nature of terrorism financing differs from that of money laundering, the risk assessment must include also an analysis of the vulnerabilities of terrorism financing. Since the funds used for terrorism financing may stem from legal sources, the nature of sources may vary. When the sources of terrorism financing originate from criminal activities, the risk assessment related to money laundering is also applicable to terrorism financing.

3. Risk identification and analysis

The first step in assessing ML/TF risks is to identify certain risk categories, i.e., customers, countries or geographical locations, products, services, transactions and delivery channels specific for the entity. Depending on the specificity of operations of an entity, other categories could be considered to identify all segments in which ML/TF risk may emerge. The significance of different risk categories may vary from entity to entity, i.e., an entity may decide that some risk categories are more important to it than others.

For the analysis, the entity should make an estimate of the likelihood that these types or categories of customers will misuse the entity for money laundering or terrorism financing. This likelihood is for instance high if it can occur several times per year, medium if it can occur once per year and low if it is unlikely, but not impossible. In assessing the impact, the entity can for instance look at the financial damages from the crime itself or from regulatory sanctions; the reputational damage to the entity or the sector. The impact can vary from minor if there are only short term or low cost consequences to (very) major when there are very costly and long term consequences that affect the proper functioning of the entity. The tables below show a three-point scale. An entity can also decide on a more detailed scale.

Rating	Likelihood
HIGH	Probably occurs several times per year
MEDIUM	Probably occurs once per year
LOW	Unlikely to occur but not impossible

Rating	Impact
MAJOR	Long term, high cost consequences affecting functioning
MODERATE	Medium term consequences with some costs
MINOR	Short term or low cost consequences

Country or geographical risk

Country or geographical risk may arise because of the location of a customer, the origin of destination of transactions of the customer, but also because of the business activities of the entity itself, its location and the location of its organisational units. Country or geographical risk, combined with other risk categories, provides useful information on potential exposure to money laundering and terrorism financing.

There is no general definition based on which particular countries or geographical areas can be categorised as low or high risk. The factors which may define if a specific country or geographical area is more vulnerable to money laundering and terrorism financing, may include different criteria. Factors that may indicate a higher risk are:

- Countries or geographic areas subject to sanctions, embargoes or comparable restrictive measures issued, for instance, by the United Nations, the European Union or the United States.
- Countries or geographic areas identified by credible sources (e.g., the FATF, the IMF or the World Bank) as lacking an appropriate system of preventing money laundering and/or terrorism financing. Reference is made to the 'ICRG process' (International Co-operation Review Group) of the FATF. After each of its meetings (held in February, June and October) the FATF publishes lists of countries which in its opinion lack an adequate system of combating money laundering and terrorism financing.
- Countries or geographic areas identified by credible sources as providing funding for or otherwise supporting terrorist activities.
- Countries or geographic areas identified by credible sources as having a high level of corruption, or other criminal activity.

Customer risk

For the purpose of the ML/TF risk assessment, the entity should define if a type of customer carries an increased ML/TF risk. Based on its own criteria, an entity will determine whether a customer poses a higher risk. Categories of customers that may indicate a higher risk are:

- Customers who conduct their business relationships or transactions (or who have these conducted) under unusual circumstances, such as an unexplained geographic distance between the entity and the location of the customer, frequent and unexplained transfers of accounts to different institutions and frequent and unexplained movements of funds between accounts in various geographic locations.
- Customers where the structure or characteristics of the entity or relationship make it difficult to identify the true owner or controlling interests, or customer that use nominees, trusts, family members or third parties, etc.
- Cash intensive businesses including (informal) money transfer agencies, bureaux de change, betting houses, gambling halls, etc.
- Charities and other 'not-for-profit' organisations (especially those operating on a 'cross-border' basis) which are not subject to any form of monitoring or supervision.
- Indirect relationships through intermediaries who are not (or not sufficiently) subject to AML/CFT measures or who are not supervised.
- Customers who are Politically Exposed Persons (PEPs).
- Occasional customers that do transactions above a certain threshold.

The delivery channels play a role when assessing the customer risk. The extent to which the entity works with customers directly or through intermediaries or correspondent institutions, or establishes business relationships without customers being physically present are important factors to be considered in assessing the risk of a category of customers.

The entity will describe all types or categories of customers that it provides business to and should make an estimate of the likelihood that these types or categories of customers will misuse the entity for money laundering or terrorism financing, and the consequent impact if indeed that occurs.

EXAMPLE ONLY

Description of types of customers

SME business:
The SME business customers usually are domestic companies with simple ownership structure. Most of these businesses deal with cash and multiple persons can be acting on their behalf. The likelihood that funds deposited are from illegitimate source is medium. Because of the large number of SME customers the impact can be major. The risk assessment is high.

International corporations:
Customers that are international corporations have complex ownership structures with often foreign beneficial ownership. Although there are only few of those customers, most are located in offshore locations. The likelihood of ML is high but because of the limited number of customer the impact will be moderate. The risk assessment is medium.
Etc., etc.

These descriptions can result in a table as below:

EXAMPLE ONLY

Type of customer	***Likelihood***	***Impact***	***Risk analysis***
Domestic retail customer	medium	moderate	medium
Private banking customer	high	major	high
SME business	high	major	high
International corporation	high	moderate	medium
Company listed on stock exchange	low	minor	low
PEP	high	major	high
Securities broker	low	high	medium
Incidental customer	high	medium	medium

The above risk analysis is a general one for types or categories of customers. It is the starting point for the risk classification of an individual customer. Based on the circumstances of an individual customer, such as its background or information provided, the risk classification of an individual customer can be adjusted. Based on that individual risk classification, customer due diligence measures will be applied.

Transaction, product and service risk

A comprehensive ML/TF risk assessment must take into account the potential risks arising from the transactions, products and services that the entity offers to its customers and the way these products and services are delivered to the customer. The entity should pay particular attention to ML/TF risk which may arise from the application of new technologies. In identifying the risks of transactions, products, and services, the following factors can be considered:

- Services identified by internationally recognised and credible sources as being a higher-risk, such as international correspondent banking services and (international) private banking activities.
- Services involving banknotes and precious metal trading and delivery.
- Services that inherently promote anonymity or can readily cross international borders, such as online banking services, prepaid cards, private investment companies and trusts.
- New or innovative products or services that are not provided directly by the entity but are provided through channels of the entity.
- Products that involve large payment or receipt in cash.
- Purchase of valuable assets or commodities (real estate, race horses, vehicles, gems, precious metals, etc.)
- Gaming activities (horse racing, internet gambling, etc.)
- Non face-to-face transactions or services
- One-off transactions

Specific lease products, life insurance policies with a low annual premium or a low single premium, consumer loans or savings products have a low inherent risk because of the long term to realise benefits. Other products, such as back-to-back loans, trade finance, real estate transactions and other high-quality, complex products may produce a higher risk because of their complexity or lack of transparency.

For the risk assessment, the entity will describe all products and services that it provides and make an estimate of the likelihood that customers will misuse that product for money laundering or financing of terrorism, and the impact thereof.

EXAMPLE ONLY

Description of types of products, transactions and services

Life insurance

The life insurance products are simple and premiums tend to be very low. Premiums can only be paid through a bank account and no cash is involved. The life insurance products are only sold to resident persons. The likelihood that insurance products are used for ML/TF is low as will be the impact if it is. Risk assessment is low.

Prepaid cards

Prepaid cards are a new product and its usage is not clear yet. Funds tend to be loaded through cash deposits and it is not necessary to have a bank account. The likelihood that prepaid cards are used for ML/TF is high and the impact on the business, seeing that it is a new product, will be very high. Risk assessment is high.
Etc., etc.

This description can result in a table as below:

EXAMPLE ONLY

Type of transaction	***Likelihood***	***Impact***	***Risk analysis***
Betting transaction	high	moderate	medium
Online transactions	high	major	high
Domestic bank transfer	medium	moderate	medium
Prepaid card	high	major	high
Life insurance	low	minor	low
Securities account	low	minor	low

4. Risk matrix

In assessing the risk of money laundering and terrorism financing, the entity is to establish whether all identified categories of risks pose a low, medium, high or unacceptable risk to the business operations. The entity must review different factors, e.g., number and scope of transactions, geographical location and nature of the business relationship. In doing so, the entity must also review the differences in the manner in which the entity establishes and maintains a business relationship with a customer (e.g., direct contact or non face-to-face). It is due to the combination of these factors and the variety of their combinations, that the level of money laundering and terrorism financing differs from entity to entity. The geographical risk should be seen in correlation with other risk factors in order to come up with an assessment of the total money laundering and terrorism financing risk. Thus, for example, a low risk product in combination with a customer from a high risk country will combined carry a higher risk.

Entities can use a risk matrix as a method of assessing risk in order to identify the types or categories of customers that are in the low-risk zone, those that carry somewhat higher, but still acceptable risk, and those that carry a high or unacceptable risk of money laundering and terrorism financing. In classifying the risk, the entity, taking into account its specificities, may also define additional levels of ML/TF risk. The development of a risk matrix can include the consideration of a wide range of risk categories, such as the products and services offered by the entity, the customers to whom the products and services are offered, the entity's size and organisational structure, etc. A risk matrix is not static: it changes as the circumstances of the entity change. A risk analysis will assist an entity to recognise that ML/TF risks may vary across customers, products, and geographic areas and thereby focus its efforts on high-risk areas in its business.

The following is an example of a risk matrix of client-product combinations that can be developed based on the risk analysis.

EXAMPLE ONLY

Transaction Customer	Betting transaction	Online transaction	Domestic transfer	Prepaid card	Life insurance	Securities account
Domestic retail customer	medium	medium	medium	medium	low	low
Private banking customer	n/a	high	medium	high	n/a	medium
SME business customer	high	high	medium	high	medium	medium
International corporation	medium	high	medium	high	medium	medium
Company listed on stock exchange	medium	medium	low	medium	low	low
PEP	high	high	medium	high	medium	medium
Securities broker	n/a	medium	medium	n/a	n/a	medium
Incidental customer	medium	high	medium	high	n/a	n/a

The entity must take care that this risk identification and analysis is properly documented in order to be able to demonstrate it as the basis of the AML/CFT policies and procedures, and to be able to provide the risk assessment information to the supervisory authorities.

5. Risk management

The ML/TF risk of each entity is specific and requires an adequate risk management approach, corresponding to the level and structure of the risk, and to the size of the entity. The objectives and principles of ML/TF risk management should enable entities to establish a business strategy, risk appetite, adequate policies and procedures, promote high ethical and professional standards and prevent entities from being misused, intentionally or unintentionally, for criminal activities.

ML/TF risk management requires attention and participation of several business units with different competences and responsibilities. It is important for each business unit to precisely know its role, level of authority and responsibility within the entity's organisational structure and within the structure of ML/TF risk management.

It is desirable for managers of different lines of business, responsible for risk management at the level of their organisational unit, to develop ML/TF risk management procedures, corresponding to the specific tasks of the organisational unit in question, which must be harmonised with the objectives and principles of ML/TF risk at the level of the entity as a whole.

Role of Management

Management gives direction to its business activities by setting the risk appetite, formulating objectives and making strategic choices from which subsequently policy and procedures are derived. Management should be able to determine the ML/TF risks of the business and take these into account in the entity's ultimate goals and strategies. Documentation and communication of strategy, policies and procedures are important for their actual implementation. Tools in this respect are, for instance, mission statements, business principles or strategic views. Management will also give direction to setting up, implementing and monitoring the ML/TF control framework and will be responsible for the strategic choices to be made and decisions to be taken in that respect.

Management should be actively involved in analysing and recognizing ML/TF risks and take adequate control measures (e.g., by allocating sufficient resources to setting up an adequate monitoring system or training). Management will thereby receive support from functions (compliance, security, risk management, commercial functions, etc.) that possess relevant knowledge and experience. Management should also determine the risk tolerance while guarding against the entity accepting customers or providing products and services on whom or which the entity has no knowledge or experience. It should ensure that sufficient account is taken of ML/TF risks in the development and pre-introduction phase of new products and services. It is important in this respect that members of the management team involved in the decision-making process have sufficient authority and powers to take and implement the necessary decisions (or have these implemented).

Management's leadership abilities in and commitment to the prevention of money laundering and terrorism financing are important aspects of implementing the risk-based approach. Management must encourage regulatory compliance and ensure that employees abide by internal procedures, policies, practices and processes aimed at risk mitigation and control. Management should also promote an ethical business culture and ethical behaviour. Ethical behaviour is a professional, individual responsibility, where individuals should be aware of the rights, interests and wishes of other stakeholders and conscientiously take them into account, have an open and transparent mind-set, and be willing to take responsibility and be held accountable for their decisions and actions. An ethical business culture denotes a climate and atmosphere in which an entity, also in a broader sense, behaves or acts in a way it can explain and account for. A culture in which this professional, individual responsibility is stimulated and rewarded, and which not only respects the letter of the law, but also its spirit. The elements underpinning this culture are: balancing of interests, balanced and consistent actions, openness to discussion, leading by example, feasibility, enforcement and transparency.

Policies and procedures

Once the identification and risk analysis processes are completed, the strategy of ML/TF risk management is applied to enable the entity to implement adequate policies and procedures for reducing the risks and bringing it down to an acceptable level, with a view to avoiding reputational risks, operational risks, risks of sanctions imposed by a regulatory body and other forms of risk.

The policies and procedures are approved by management and are applicable to all business units, branches and majority-owned subsidiaries. They should allow for sharing of information between business units, branches and majority-owned subsidiaries, with adequate safeguards on confidentiality and use of information exchanged. By assessing the risks and developing policies and procedures the entity ensures the continuity of ML/TF risk management controls despite any changes in the management or staff composition or structure.

The policies and procedures should enable the entity to effectively manage and mitigate the identified risks and focus its efforts on areas in its business which are more vulnerable to ML/TF misuse. The higher the risk, the more control measures have to be applied. An entity can implement adequate ML/TF risk controls for higher risk products by setting transaction limits and/or a management approval escalation process. Also, the development and application of risk categories for customers together with customer due diligence and transaction monitoring measures based on those risk categories is one of the strategies for managing potential ML/TF risks posed by customers. Specific policies and procedures will therefore need to be developed with respect to customer due diligence, transaction monitoring, recordkeeping and reporting to the FIU.

6. Risk monitoring and review

Management should be able to adequately manage ML/TF risks, to verify the level of implementation and functioning of the ML/TF risk controls, and to ascertain that the risk management measures correspond to the entity's risk analysis. The entity should therefore establish an appropriate and continuing process for ML/TF risk monitoring and review. This process will be done by the business control function to ensure on a regular basis that all processes are implemented; the compliance function to periodically monitor if the policies are adhered to and systems are in place; and the audit function to assess if the policies and process are conform the law and are performed in an adequate way.

Monitoring process

Regular reports to management should contain the results of the monitoring process, findings of internal controls, reports of organisational units in charge of compliance and risk management, reports of internal auditing, reports of the person authorised for detecting, monitoring and reporting any suspicious transactions to the FIU, as well as the findings contained in the supervisor's inspection reports on AML/CFT. Management should be furnished with all important information which will enable it to verify the level AML/CFT controls, as well as possible consequences for the entity's business if controls are not functioning properly.

The risk reports should indicate if appropriate control measures are established and adequate and fully implemented for the entity to protect itself from possible ML/TF misuse. The monitoring and review process should include the appraisal of ML/TF risk exposure for all customers, products and activities, and ensure the implementation of proper control systems, with a view to identifying and indicating problems before any negative consequences for the entity's business occur. This process may also alert the entity to any potential failures, for instance failure to include mandatory legislative components in the policies and procedures, insufficient or inappropriate customer due diligence, or level of risk awareness not aligned with potential exposure to ML/TF risks.

Review of the ML/TF risk assessment

The entity must keep the ML/TF risk assessment up to date by setting up and describing the process of periodically reviewing the risk assessment. The entity must therefore also stay up-to-date with ML/TF methods and trends, international developments in the area of AML/CFT, and domestic legislation. Such a review can also include an assessment of the risk management resources such as funding and staff allocation and may also identify any future needs relevant to the nature, size and complexity of the entity's business.

A review should also be conducted when the business strategy or risk appetite of an entity changes or when deficiencies in the effectiveness are detected. When the entity is to introduce a new product or activity, an ML/TF risk analysis of that product is to be conducted before offering that new product or activity to customers.

Steps to be taken for the ML/TF risk assessment

Identifying risks

- What is the size and nature of the business?
- Identify aspects of the business that can be susceptible to ML/TF.
  - What type of clients, product and services does the entity has?
  - What kind of delivery channels are used for the products and services?
- What countries does the entity or its customers do business in?

Analysing risks

- Determine per type of client or product the likelihood that ML/TF occurs.
  - Consider factors as cash intensive products, frequent international transactions, complex corporate customers.
  - If ML/TF can occur several times per year, the likelihood will be high.
- Estimate the impact if the risk happened.
  - Consider cost of crime itself, but also from possible fines or enhanced mitigation efforts and loss of reputation.
  - If the amount of loss, damamges or cost is high, the impact will be major.

Risk matrix

- Develop a risk matrix to ascertain which client-product combinations pose higher ML/TF risks.
- Establish whether the delivery channels pose an additional higher ML/TF risk factor.
- Establish whether country risk is an overall higher ML/TF risk factor.

Risk management

- Based on the analysis set the overall AML/CFT strategy.
  - Consider if the strategy concurs with the risk appetite and risk culture.
  - Ensure that management clearly promotes AML/CFT the strategy and sets the tone.
- Develop an AML/CFT policy, procedures and mitigating measures.
  - Determine for which measures will be taken for which risk categories.
  - Ensure sufficient training for staff in AML/CFT policies and procedures.
  - Provide tools and systems to implement the AML/CFT system.

Monitoring and review

- Set up compliance monitoring and audit program.
  - Regularly test if the procedures and measures are working correctly.
  - Provide regular compliance and audit reports to management.
- Review the risk assessment.
  - Are there new product or business lines?
  - Has the legislative framework changed?
  - Is the business expanding into new areas or countries?