
Public Compliance Communication
Risk Based Supervision Framework.

This Public Compliance provides guidance to sector supervisors on the drafting of a risk-based compliance framework when performing their supervision duties in line with regulation 18 of the Money Laundering and Proceeds of Crime Regulations, 2019.

It is guidance on how to conduct money laundering and terrorism financing (ML/TF) institutional risk assessment for anti-money laundering/counter financing of terrorism (AML/CFT) supervisors. The guidance was created to assist AML/CFT supervisors in developing data collection tools and risk assessment matrices to attribute an ML/TF risk rating to individual accountable institutions.

Information in this guideline is intended to provide general direction only and does not constitute requirements or the only approach to conducting institutional risk assessment. It is meant to provide AML/CFT supervisors with support in developing risk assessment tools to conduct an institutional risk assessment that will rest in a broader risk assessment function recognizing that an understanding of ML/TF risk at the individual obliged entity level is a critical component of implementing a risk based supervisory approach.

1. Implementing a Risk Based Approach to Supervision

A risk-based supervisory approach is a prescribed requirement of the Financial Action Task Force (FATF) standards and is also recognized as best practice internationally. It has become evident that most supervisory authorities have limited resources, and therefore the risk-based supervisory approach permits authorities to determine which supervisory activities are the most appropriate and applicable. This is determined according to the non-compliance risk exposure of money laundering and terrorism financing that is present within a sector and respective accountable institutions.

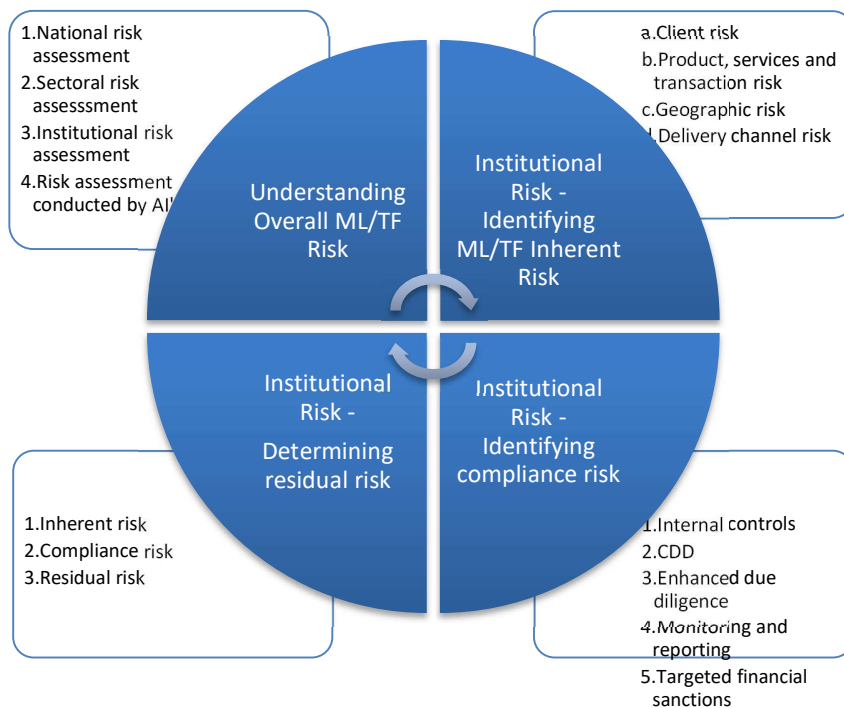
A risk-based supervisory approach presents several strategic advantages. It aims to focus these limited supervisory resources to the highest risk areas and institutions. This targeted approach aims to achieve the highest level of compliance with strategic allocation of resources. When a comprehensive risk-based supervision is efficiently applied it should result in majority institutions being compliant with their obligations and higher risk institutions being subject to more probing supervision and corrective actions than their lower risk counterparts.

A risk-based approach must be integrated in all aspects of a supervisory framework design. As the AML/CFT supervisor develops its supervisory framework, a risk-based approach is integrated in all elements of the framework design. It should serve as the lens by which all supervisory activities are conducted.

Understanding ML/TF risk at the institutional level allows AML/CFT supervisors to orient their limited resources towards the entities that are at highest risk of ML/TF or non-compliance. An institutional risk assessment allows the AML/CFT supervisor to allocate a risk score to each obliged entity while gaining an understanding of what clients, products, services, transactions, geographic areas and delivery channels are at highest risk of being exploited by money launderers and terrorist financiers.

Below is a 4-step process to assessing ML/TF institutional risk. The process outlines the following four steps to understanding institutional risk:

1. Understanding Overall ML/TF Risk
2. Identifying ML/TF Risks
3. Identifying compliance risk
4. Determining residual risk



2. UNDERSTANDING OVERALL Money Laundering and Terrorist Financing Risk

2.1 Different types of ML/TF risk assessment

Before developing risk assessment tools to assess institutional risk the supervisory authority should understand the ML/TF risk environment in which it operates. It should consider the various risk assessment exercises that are undertaken under the AML/CFT framework notably:

- a. **The National Risk Assessment (NRA)** the assessment of national threats and vulnerabilities undertaken by all AML/CFT competent authorities and the private sector.
- b. **The Sectoral Risk Assessment** which evaluates the risk of each obligated sector and helps allocate supervisory resources. In most countries, the sectoral risk assessment has been conducted in the context of the NRA by the relevant supervisory authority with feedback by the private sector.

The sectoral risk assessment will provide insights as to which sectors are higher risks of ML/TF and should identify the types of clients, products, services, geographic locations, and delivery channels that are most vulnerable to ML/TF for each sector. The inherent vulnerabilities identified in the sectoral risk assessment will serve as the basis for establishing the risk assessment criteria that will serve as the heart of the institutional risk assessment. Finally, the risk assessments conducted by AI's will provide additional information and validate the types of vulnerabilities that can be exploited by money launderers, criminals and terrorist financiers and that should therefore be considered when conducting an institutional risk assessment.

- c. **The Institutional Risk Assessment** which evaluates the risk of individual entities and helps supervisory authorities target highest risk entities. The institutional risk assessment is conducted by the supervisory authority based on information gathered through a

statistical questionnaire as well as information from all the other types of risk assessment.

The institutional risk assessment considers information from the other types of risk assessment to determine the risk level of individual reporting entities. The National Risk Assessment will provide general information on the national threats and vulnerabilities that exist including the specific threats that may be present in the sector where the institutional risk assessment is being conducted.

d. **The risk assessment conducted by the reporting entity** where individual entities assess the risk of their operations.

3. INSTITUTIONAL RISK ASSESSMENT - ASSESSING ML/TF INHERENT RISK

Sector specific statistical questionnaires and risk matrices to evaluate the risk of individual accountable institutions is a crucial step in adopting a comprehensive risk-based supervisory framework. Once the sectoral risk assessment has been completed an analysis of which accountable institutions (AIs) are at highest risk must be undertaken. This risk assessment exercise is targeted to the specificities of each designated non-financial business and profession (DNFBP) sector. Initially information to populate the risk matrices may be unavailable.

The institutional risk assessment should be based on information regarding the entity's organizational and financial factors, their client profiles, products, services and transactions risk as well geographic and delivery channel risk. This information is typically gathered through a statistical questionnaire that is administered to AIs on a regular basis although information related to inherent risk can also be obtained through other supervisory information, for instance, the licensing supervisory activities/or requirements or public information.

Statistical questionnaires are an efficient tool to gather important compliance information while also raising awareness amongst AIs. The questionnaire is administered to AIs. The sector specific statistical questionnaire gathers information that is specific to each sectors' risk profile. As with all risk assessments the evaluation of risk is continuously informed by off-site monitoring and on-site inspections as well as publicly available information.

3.1 Developing a Statistical Questionnaire

Statistical questionnaires are often the most efficient way of gathering information related to ML/TF risk. All ML/TF risk information can be gathered in one document and easily transferred into a sector specific risk matrix.

The first step in establishing an ML/TF statistical questionnaire is to determine which assessment criteria the supervisory body wants to establish to assess ML/TF risk for a sector.

As illustrated above the risk assessment criteria should help assess risks related to:

- Organizational and financial factors
- Client profile
- Products, services and transactions
- Geography, and
- Delivery channels

The following paragraphs will outline possible risk assessment criteria/factors that supervisory bodies may want to consider when developing their statistical questionnaire that will help populate their risk assessment matrix. The risk assessment criteria should be based on both national and sectoral specificities and risk assessments. It is important to note that the risk assessment criteria listed below are not exhaustive and supervisory authorities should develop a comprehensive list of risk assessment criteria based on a sector's identified ML/TF risk factors.

➤ **Assessing organizational and financial factors**

In understanding an AI's risk profile certain organizational and financial factors contribute to an entity being at higher risk of ML/TF. These may include:

- The volume of transactions
- The total value of transactions conducted
- The complexity of the entity's organizational structure
- List of other sector specific risk factors

➤ **Assessing risks related to client profile**

In understanding an entity's risk profile certain types of clients contribute to an entity being at higher risk of ML/TF. These might include:

- Politically Exposed Persons
- Clients involving complex ownership structures
- Clients acting on behalf of third parties
- High net worth clients
- List of other sector specific risk factors

➤ **Assessing products, services, transactions**

The assessment of products, services and transactions will be specific to each sector. The national and sectoral risk assessment may assist in highlighting which products have been picked up as more vulnerable to ML/TF.

For example, for accountants the following activities could be considered higher risk given that they have been designated by the FATF in Recommendation 22¹:

- Real estate transactions
- Managing of client money, securities or other assets
- Management of bank, savings or securities accounts
- Organizing or managing contributions for creation, operation or management of legal persons
- Creation, operation and management of legal persons
- Purchase and sale of business entities

Assessing geographic risk

In understanding an entity's risk profile, the involvement of certain geographic areas or countries contribute to an entity being at higher risk of ML/TF. These might include:


- Countries identified by FATF or FSRB as being higher risk
- United Nations sanctioned countries
- Illegal Drugs producing countries
- Countries with known links to terrorism
- List of other sector specific risk factors
- An AI with branches in High Risk districts
- An AI with branches located next to the Boarder gates.
- Countries allowing shells banks to operate in their jurisdiction
- Countries which allow nominee shareholding or nominee directors
- Countries which allow bearer shares or bearer share warrants

¹ INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND FINANCING OF TERRORISM AND PROLIFERATION (FATF RECOMMENDATIONS)

Assessing delivery channel risk

In understanding an entity's risk profile how an AI delivers its services (delivery channels) can contribute to an entity being at higher risk of ML/TF. These may include:

- Transactions/activities that are not conducted face-to-face
- A predominantly cash based activity
- Transactions/activities that are conducted by proxy
- List of other sector specific risk factors
- Cross border transactions

 **Annex A provides a general template of how a statically questionnaire could be organized.**

3.2 Developing Sector Specific ML/TF Risk Assessment Matrices

An ML/TF risk assessment matrix should be developed for each sector subject to AML/CFT obligations. Once a supervisory authority has established the risk assessment criteria for each sector it supervises, it will need to develop a sector specific risk matrix. The sector specific ML/TF Risk Matrix will assist supervisory authority in assessing ML/TF Inherent Risk, Compliance Risk as well as Residual Risk (see following chapters).

A rating scale should be established to evaluate the risk assessment criteria. A simple rating scale will attribute low (rating score of 1), moderate (rating score of 2) or high (rating score of 3). Supervisory authorities that want a more graduated risk can adopt a 5-point risk scale: low (1), medium-low (2), medium (3), medium-high (4) and high (5). If choosing a more graduated risk scale the supervisory authority should ensure that it has sufficiently precise risk information to populate its risk matrix.

Table 3.2.1 . Three-Point Rating Scale

Compliance Risk Rating Scale	
a) Low risk	1
b) Moderate risk	2
c) High risk	3

A risk rating should be attributed to each risk assessment criteria based on the established risk scale. For each range of answers provided a risk score should be established. It is important to note that the risk range will vary according to the specificities of each sector such as the size and the volume of transactions. An example of a risk range might include using a 3- point scale of low (1), medium (2) and high (3) to evaluate risk as follows:

Example 3.2.1. Establishing a rating range and rating scale

Client Profile	Inherent Risk Rating
Are certain of your clients politically exposed persons	
Politically exposed persons?	
a) 0	1
b) Between 1 and 5	2
c) Over 5	3

The risk assessment matrix should also attribute a weight to each risk assessment criteria. Some risk assessment criteria will be considered more important than others. The supervisory body can attribute a weight of **0.5** for risk assessment criteria that are deemed less important, **1** for risk assessment criteria that are deemed important and a weight of **2** for assessment criteria that are deemed very important. The weight is multiplied with the risk rating to arrive at a risk score for the risk criteria.

Diagram 3.2.1. Calculating risk score for risk criteria



The example below provides an example of different weights being attributed to risk assessment criteria. In this example, the risk assessment criteria measuring the value of transactions (or annual turnover) conducted by an entity is rated a very important (weight of 2) given that it determines how much money can be potentially laundered by the entity in contrast to the number of transactions conducted by the entity which is rated important (weight of 1) versus the number of employees which is deemed relatively less important (weight of 0.5). It should be noted that this is presented as an example and that supervisory authorities may arrive at a different weight determination based on context of their sector.

Example 3.2.2. Attributing Weight to Inherent Risk Assessment Criteria

Organizational and Financial Risk			
Risk Assessment Criteria	Risk Rating	Weight	Risk Score
Annual revenue related to the buying and selling of real estate		2	
a) over M5,000,000	3		6
b) between M1,000,000 and M5,000,000	2		4
c) below M1,000,000	1		2

Number of employees		0.5	
a) more than 10	3		1.5
b) between 5 - 10 employees	2		1
c) less than 5	1		0.5
Number of real estate transactions (buying and selling) conducted annually		1	
a) more than 30	3		3
b) between 10 - 30	2		2
c) less than 10	1		1

The overall ML/TF Inherent Risk is then calculated based on adding the risk score for each inherent risk criteria. To facilitate the comparison on inherent risk scores a risk percentage can be calculated by dividing the overall risk score with the baseline for highest risk.

4. INSTITUTIONAL RISK ASSESSMENT - ASSESSING COMPLIANCE RISK

The assessment of compliance risk will determine whether an entity's mitigation measures are effective. The determination of the effectiveness of mitigation measures or controls is first to determine whether the entity is complying with its AML/CFT obligations. In addition, a supervisory body will want to determine whether the entity's **policies** and **procedures** adequately mitigate the ML/TF risks that have been identified for the entity.

The determination of compliance risk assessment criteria is based on the list of requirements that are imposed on the AI. The supervisory authority can frame the risk assessment criteria broadly for example by list of AML/CFT obligations.

Compliance risk assessment criteria may be framed as follows:

- Development and implementation of internal controls and policies and procedures,
- Development of ML/TF risk assessment,

- Implementation of risk mitigation measures,
- Conduct of internal audit,
- Conduct of AML/CFT trainings
- KYC requirements on onboarding
- Implementation of customer due diligence (CDD) measures
- Implementation of record keeping measures
- Implementation of enhanced due diligence (EDD) measures for high-risk clientele
- Implementation of ongoing monitoring measures
- Implementation of a mechanism to identify and report suspicious transaction reports
- Implementation of a mechanism to monitor targeted financial sanctions (as designated by the United Nations or a national authority)
- Effective mitigation of ML/TF risk

A rating scale should be established to evaluate compliance risk. The rating scale will be informed by the rating scale selected to evaluate inherent ML/TF risk. If a 3-point rating scale was selected to evaluate the ML/TF inherent risk a 3-point rating scale will also need to be selected to assess compliance risk.

A compliance rating scale wants to give AI's credit for effectively implementing their AML/CFT obligations. As such a higher compliance risk score means that the AI is effectively implementing its AML/CFT obligations and reducing the likelihood that the entity will be used for ML/TF in contrast with a higher ML/TF inherent risk score which signifies that the AI is more susceptible to being used for ML/TF.

A compliance risk rating scale may be structured as follows:

Compliance Risk Rating Scale (Example)	
a) Low level of compliance	1
b) Moderate level of compliance	2
c) High level of compliance	3

A weight should be attributed to each compliance risk assessment criteria. As when evaluating inherent ML/TF risk some compliance risk assessment criteria will be considered more important than others. The supervisory authority can attribute a weight of 0.5 for risk assessment criteria that are deemed less

important, 1 for risk assessment criteria that are deemed important and a weight of 2 for assessment criteria that are deemed very important. The weight is multiplied with the risk rating to arrive at a compliance risk score



4.1 Methods to determine compliance risk

Supervisors can assess compliance risk through the results of monitoring and inspections or through the AI's self-assessment.

The most accurate way to assess the level of compliance risk is to conduct monitoring and inspection activities. Supervisors are in the best position to determine whether AI's are effectively implementing their AML/CFT

obligations. As such, when monitoring or inspection results are available, they should be used to determine the level of compliance risk.

In absence of monitoring or inspection results, AP's self-assessments through statistical questionnaires can be used to assess compliance risk. The statistical questionnaire can ask entities whether they are complying with AML/CFT obligations by listing the main categories of obligations as identified previously in this chapter. Although it will provide supervisory authorities with some information on whether AML/CFT obligations are being complied with the ratings will not be as accurate as those derived from monitoring and inspection findings.

INSTITUTIONAL RISK ASSESSMENT - ASSESSING RESIDUAL RISK

ML/TF residual risk will be calculated based on the inherent ML/TF risk and compliance risk scores. The compliance risk score will be subtracted from the inherent ML/TF risk score. This residual risk calculation sees AP's obtain a reduced ML/TF residual risk when they effectively implement their AML/CFT obligations,

Diagram 5.1. Calculating ML/TF Residual Risk



6. KEEPING INSTITUTIONAL RISK ASSESSMENT UP TO DATE

The institutional risk assessment should be updated regularly. The supervisory body should update its inherent ML/TF risk assessment on a 1 to 3-year cycle to ensure that institutional risk assessments are based on current information. In selecting the risk assessment cycle the supervisory body should consider a sector's sectoral risk assessment with higher risk sectors being subject to a more frequent institutional risk assessment cycle.

The number of entities in a sector may also impact the frequency of the institutional risk assessment cycle with larger sectors being subject to a review of their AP risk assessment less frequently.

Update of the compliance risk assessment. The compliance risk assessment should be updated every time a monitoring or inspection activity is undertaken. The compliance risk assessment should not be updated until another monitoring or inspection activity is undertaken. When no monitoring or inspection activity has been undertaken the supervisory body can rely on the latest self-assessment provided by the entity through the statistical questionnaire.

Annex A. Structure for ML/TF Statistical Questionnaire

I - GENERAL INFORMATION

1. Name of firm

--

2. Date questionnaire was completed:

3. Name(s) of CEO or owner:

--

4. Name of Compliance Officer:

--

5. When was your firm/entity last subject to an AML/CFT audit (provide date):

--

II - FIRM STRUCTURE AND FINANCIAL FACTORS

1. FIRM STRUCTURE

Risk assessment criteria	
Risk assessment criteria	
Risk assessment criteria	

2. FINANCIAL FACTORS

Risk assessment criteria	
Risk assessment criteria	
Risk assessment criteria	

INHERENT RISKS

1. CLIENT RISK	No clients	Value of transasacti ons
Risk assessment criteria		

Risk assessment criteria		
Risk assessment criteria		

2. PRODUCTS, SERVICES AND TRANSACTION RISK (services provided for clients)	No. of Transactions	Total transaction value (Maloti Equivalent)
Risk assessment criteria		
Risk assessment criteria		
Risk assessment criteria		

3. GEOGRAPHIC RISK (See Guideline on AML/CFT Obligations for Real Estate)	No. Clients	Value of transactions
Risk assessment criteria		
Risk assessment criteria		
Risk assessment criteria		

4. CHANNELS OF DELIVERY RISK	No. Clients	Transaction value (Maloti)
Risk assessment criteria		
Risk assessment criteria		
Risk assessment criteria		

5. IMPLEMENTATION OF AML/CFT OBLIGATIONS	YES/PARTIALLY/NO
Risk assessment criteria	
Risk assessment criteria	
Risk assessment criteria	