RISK SCORING MODELS

A risk scoring model can be used with numeric values to determine the category of risk for each inherent risk factor (customers, products, channels and service providers, geography).
For example: -

a) Simple 3 element model for risk scoring scale (Low, Medium and High)

In a simple three element model all three categories are combined to get a composite score. Care must be taken not to advertently discount any element that is an outlier from other elements.
If the risk factor is 3 for each element then the aggregate score would be 9. However, if two of the elements have a score of 1 and the other has 7 then the composite score is 9 and there is need to identify how and what manner the element scoring 7 should be mitigated. This could mean implementing a more rigorous control or introducing restrictions.
When categories are combined the customer risk picture becomes clearer. For example, when you combine a product with the customer type the combination can radically change the level of risk.

b) Sophisticated Model

Creates combinations of factors (customer, product of customer, geography, service delivery and channels) that will determine the overall rating).

CUSTOMER TYPE	PRODUCT/ SERVICE DELIVERY	GEOGRAPHY	COMPOSITE SCORE	RISK SCORE Obtain average
Foreign private company	Checking account with online transfers capabilities	High risk jurisdictions		
9	9	9	27	9 (High)
PEP or foreigner	Private banking	USA		
7	7	3	17	5.3 (Medium Risk)
Public company	Retirement account	Somalia		3 (Low)
1	1	7	9	3 (Low)

For the public company the customer and product will have a much lower risk
Then, a likelihood score is assigned to each risk factor based on the Likelihood Scores Index (Table 1 – Likelihood Scores Index) and the respective risk rating is assigned

(Table 2 – Risk Classification).

Table 1 – Likelihood Scores Index

SCORE	INDEX
0	No likelihood of the event occurring
1	Rare, occurs only in exceptional circumstances
2	Unlikely, may occur at some point
3	Possible, likely that the event will occur at some point

4	Likely, the event is likely to occur in most cases
5	Very Likely, the occurrence of the event is considered as normal

Table 2 – Risk Classification

RISK CLASSIFICATION	LOW	MEDIUM	HIGH
RISK SCORE	0 – 1	2 – 3	4 – 5
INDICATION	Low probability that the risk is present	Probable that the risk is present	High probability that the risk is present

Reporting entities/ accountable person may use the AML/CFT Institutional Risk Assessment Template to assess their institutional risk. Please note that it is not mandatory for reporting entities/accountable person to use the template or the risk model outlined as long as the reporting entity/accountable person is able to effectively demonstrate its risk assessment methodology and that it has taken reasonable measures to identify and assess its risks.

IMPLEMENTING AND EVALUATING THE AML/CFT INTERNAL CONTROLS

Once the reporting entity/accountable person has identified its ML/TF risk exposure, internal controls must be implemented and evaluated to determine how effectively they offset the identified risks. Controls are programs, policies or activities put in place by reporting entities/accountable person to prevent their businesses from being used to facilitate ML /TF, or to ensure that potential risks are promptly identified and mitigated accordingly.

There are a number of controls which can be implemented to mitigate the identified risks, some of which, are a regulatory requirement as per the AML/CFT laws, and as such, are also used to maintain compliance with the AML/CFT regulatory requirements.

As part of the risk assessment process, the internal controls implemented should be periodically reviewed and tested for effectiveness to verify whether any amendments are required in light of any emerging risks or change in existing risks identified by the reporting entity/accountable person.

Stated here-under, but not limited to, are examples of control measures that can be implemented by reporting entity/accountable person to mitigate identified risk.

i) Implementation of AML/CFT Programme

The risk assessment should enable you to prepare a comprehensive AML/CFT programme and meet your obligations under the AML/CFT Act, including procedures for the application of customer due diligence, monitoring of customer transactions and reporting of suspicious activities. Although the policies and procedures implemented must meet the minimum requirements prescribed by the legislations, the mitigation measures must be commensurate with the level and type of risks faced by the reporting entity/accountable person.

ii) Compliance Officer Function

The Compliance Officer has the over-arching responsibility to ensure that the AML/CFT measures established by the reporting entity/accountable person are being implemented effectively. Whilst assessing its risks, reporting entities/accountable person are able to obtain a broad view of its customer profiles, the volume and type of businesses (services/ products), volume and type of transactions routing through it and the potential ML/TF risks to the business. As the business' level of complexity, size and risk increases, the risk assessment should help AML/CFT Institutional Risk Assessment Guidelines in determining whether the resources being allocated to its compliance function is sufficient to continuously meet its regulatory obligations (e.g should the Compliance Officer continue discharging additional duties other than the compliance function, should additional staff be employed in the compliance function, etc).

iii) Applying appropriate Customer Due Diligence (CDD) measures

Policies and procedures can be implemented to determine the level of CDD required for a particular category(ies) of customer, including PEPs based on the extent of the risks being identified. For example, an individual customer whose transaction method is solely through the use of banking facilities may pose a lower ML/TF risk compared to a non-face-face customer originating from a high-risk jurisdiction. As such, the lower risk customer may be subjected to a simplified due diligence process, while the high-risk customer may be subjected to an enhanced due diligence (EDD) process.

Section 6 (12) and (14) of the AMLA 2013 (as amended) and Regulation 14, 15 of the AMLA regulations, 2015 outlines the measures which are required to be undertaken in the application of simplified and enhanced customer due diligence requirements.

iv) Effective mechanism to monitor transactions and Reporting of Suspicious Transactions

The risk assessment will assist you in determining the triggers, red flags or scenarios which will require more in-depth scrutiny or additional information from a customer. Staff (where applicable) should be provided with adequate awareness on policies, procedures and risk identification skills to enable them to identify the triggers and red flags, and subsequently enable the effective implementation of the established policies and procedures. This will also improve the quality of monitoring and determination of whether an activity or a transaction may be deemed as suspicious based on the understanding of its customers.

4.4. Documenting the Risk Assessment Results

In accordance with Regulation 8(2) of the AML Regulations, accountable persons are required to document the results of the risk assessment and make the results available to appropriate competent authorities and regulator/supervisor and a copy shall be shared with FIA within 48 hours after conducting the risk assessment.

The results of the risk assessment and any measures undertaken by the reporting entity/accountable person to mitigate the identified risks should be consolidated within a comprehensive report and communicated to the Company's Directors, Partners or Senior Management (as applicable) to assist them in making informed decisions on the strategic direction of the company and business.

Once the risk assessment result is documented, the reporting entity/accountable person should ensure that:

a) The risk assessment is approved by Senior Management Officials such as the Directors, Partners or Owners of the Business;
b) Policies and procedures established to mitigate the identified risks are implemented effectively by the business and its staff; and
c) Ensure that all directors, partners, managers and employees (as the case may be) are adequately informed and trained on the relevant policies and procedures implemented.

REVIEW AND UPDATE OF THE RISK ASSESSMENT

Regulation 8(7) of the AML regulations, 2015 requires reporting entities/ accountable person to update its risk assessment policies, controls and procedures whenever necessary, considering the changes in its business such as entry into new markets or introduction of new products, services and technologies.

The risk assessments therefore should be updated regularly, preferably annually.

The level of ML/TF risk to which a reporting entity/accountable person is exposed to, will continuously change (either increase or decrease) depending on its nature and purpose of business, its customers' profile, the services/products it offers, and the manner in which these services/products are offered to its customers.

As such, to ensure that the reporting entity's/accountable person understanding of its risks remains current and up to date, reporting entities/accountable person should ensure that the ML/TF risk assessment is performed at least on an annual basis to ensure that any changes within the company's business model and strategy is taken into consideration within the risk assessment. This includes changes in:

a) The type or categories of customers which the reporting entity/accountable person provides services/products to;
b) The type of services or products being offered to customers;
c) The manner in which services and products are provided (i.e. delivery channels) to customers;
d) The transaction methods used by customers; and
e) New or emerging risks identified in the National Risk Assessment or through Trends & Typology reports published by the FIA, that may significantly change the risk profile of reporting entities/accountable person.

A comprehensive risk assessment also includes the assessment of the residual risks i.e., the risks after the AML/CFT internal controls have been implemented. It assists in determining how effective the controls implemented are at mitigating the identified risks. However, this is not a required component of the risk assessment. Should reporting entities/accountable person wish to assess its residual risk as part of its risk assessment, it should ensure that it is able to demonstrate how it arrived at the residual risk ratings.

ELEMENTS OF A SOUND RISK ASSESSMENT

The key elements of a credible risk assessment are;

i. The risk assessment should be documented.
ii. The risk assessment should be commensurate to the nature size and complexity of the business, profession or entity.
iii. The risk assessment should be approved by senior management and give the basis of development of policies, procedures to mitigate the ML risk.
iv. Proper governance structures should be put in place for example the risk management policies and procedures should be approved by the Board and the Board needs to oversee the policies of risk.
v. The Board of directors should have a clear understanding of the risks that the entities are exposed to and understand how the AML/CFT control framework operates to mitigate the risks.
vi. Information about the ML/TF risks assessment should be communicated to the Board in understandable, timely and accurate manner.