Notes on Customer risk assessments

This guidance note is intended to provide some further information in relation to undertaking customer risk assessments. This document is written to supplement the guidance that is provided in section 3.3 of the Anti-Money Laundering and Countering the Financing of Terrorism ("AML/CFT") Handbook.

1. What are the general customer risk assessment requirements?

A customer risk assessment must be undertaken by a regulated entity prior to the establishment of a business relationship or carrying out an occasional transaction, with, or for, that customer in order to estimate the risk of money laundering / financing of terrorism ("ML/FT") posed by a customer. This risk assessment must be documented.

The customer risk assessment should take into account that not all customer due diligence ("CDD") and relationship information might have been collected yet. It should be a living document that is revisited as more information about the customer and relationship is determined.

2. What type of customers must be high risk?

The AML/CFT Code mandates certain circumstances where a customer must be rated as high risk. This is in paragraph 15 (4) of the AML/CFT Code which states:

Matters that pose a higher risk of ML/FT include but are not restricted to –

(a) A business relationship or occasional transaction with a customer located in a jurisdiction in List A[1]; and
(b) A customer that is the subject of a warning in relation to AML/CFT matters issued by a competent authority or equivalent authority in another jurisdiction.

Where a customer is assessed as high risk enhanced due diligence ("EDD") must be obtained.

3. What type of customers may be high risk?

Apart from the aforementioned legislative requirement, the IOMFSA does not set out in guidance what types or nature of customers **must** be high risk, rather what factors should be considered in determining whether a customer **may** pose a higher risk, which are derived from the AML/CFT Code.

It is for regulated entities to formulate their own risk policies and risk appetite. The IOMFSA may review entities' risk methodologies on supervisory visits to ensure they take into account those factors referred to above and support the risk ratings that have been derived at customer level (for example through sample testing).

[1] List A specifies jurisdictions regarding which the FATF (or a FATF-style regional body) has made a call upon its members to apply counter-measures to protect the international financial system from the on-going and substantial risks of ML/FT emanating from that jurisdiction. List A can be found in the AML/CFT Handbook at Appendix D.

4. What factors should be considered in a customer risk assessment?

When assessing the ML/FT risk posed by a customer, a regulated entity should consider all known risk factors and include these in the customer's risk profile, making sure that any mitigating factors are documented accordingly.

Some examples of what the customer risk assessment must take into account include:

- The regulated entities' business risk assessment in relation to AML/CFT and their risk appetite;
- The nature, scale, complexity and geographical location of the customer's activities. This should involve looking at the sector of business the customer is involved in, whether the nature of their business puts them at a higher risk of criminal activity such as bribery or corruption, the value and complexity of transactions etc.;
- The persons to whom the customer is providing products and services to and the manner in which they are being provided. In relation to who the services are being provided to, this should examine the types of customers and understanding the rationale for providing particular products and services to these customers. In relation to the customer's offering of products and services the regulated entity should consider the extent to which they are vulnerable to ML/FT abuse, how the products and services are delivered and the value and complexity of transactions etc.; and,
- Whether there is any reliance placed on third parties for the customer due diligence process for example the use of an eligibly introduced relationship.

5. What risk rating should be assigned to a Politically Exposed Person ("PEP")?

Being identified as a PEP is a risk factor that must be considered when undertaking the customer risk assessment, however it does not automatically mean that an individual should be classed as posing a higher risk of ML/FT. It is up to the regulated entity to determine whether that particular customer should be treated as high risk depending on the customer risk assessment process and the entities' risk appetite.

The risk rating allocated to a PEP determines the extent of additional CDD, EDD and enhanced monitoring that is required to be undertaken by the regulated entity at the onset, and throughout the customer relationship.

In relation to ***any foreign PEP***, and ***higher risk domestic PEPs***, enhanced monitoring of the business relationship must be undertaken. This includes examining all aspects of the business relationship including the customer due diligence / enhanced due diligence obtained and the customer's activity. In particular it should focus on any changes in transactional activity or any transactional activity that is not in line with the customer's expected activity; these transactions should be scrutinised more thoroughly. Appropriate screening for negative press should also be undertaken.

When a PEP is assessed as posing a high risk EDD must be undertaken in addition to any requirements imposed on certain PEPs as explained above.

6. **Does the IOMFSA prescribe risk ratings for specific business or industry sectors?**

It is not IOMFSA policy to prescribe, or require regulated entities to assign, a particular risk rating to a sector or industry. Whether a customer from, or with exposure to, a particular sector would have a higher risk rating would depend on the regulated entities' customer risk assessment process and risk appetite, taking into account the extent to which a sector may be vulnerable to ML/FT abuse.

7. **Does the IOMFSA set the level of risk appetite a regulated entity should have?**

As covered above, the IOMFSA provides some guidance in the AML/CFT Handbook regarding some of the factors that should be considered by licenceholders when undertaking a business risk assessment, and as part of a customer risk assessment framework. Apart from the legislative requirements that ***require*** a customer to be assessed as high risk, the IOMFSA does not generally mandate which customers or sectors must be high risk.

A regulated entity must have documented procedures in relation to both risk assessing customers and also its risk appetite. An entity's risk appetite is likely to be based on the findings of their AML/CFT business risk assessment. Examples of what this assessment must consider include:

- The nature, scale and complexity of its business activities;
- Who its customers are and the products and services it provides;
- The manner in which it provides these products and services to its customers; and
- Whether any reliance placed on third parties for elements of CDD collected.

Also, it should be noted that there may be group-wide policies in place which could dictate a local entity's policy and risk appetite.

8. **Does the IOMFSA permit regulated entities to have high risk customers?**

The IOMFSA does not have any objection to a regulated entity having higher risk customers, provided that they have been adequately risk rated in accordance with the regulated entities' procedures and any mitigating factors have been documented. The regulated entities' risk appetite must also be considered.

Where a customer has been identified as posing a higher risk of ML/FT and the regulated entity is not satisfied it is able to effectively mitigate those risks, the regulated entity may consider the prospective customer to be of "unacceptable risk" and decline from entering into the business relationship.

Where any customer is rated as high risk EDD must be obtained.

9. **What is enhanced due diligence, and how does it impact on "de-risking"?**

If a customer is assessed as being high risk the relationship can still proceed, however EDD must be obtained. EDD is to be undertaken when any new business relationship, occasional transaction, or a continuing business relationship is assessed as posing a higher risk of ML/FT,

or when unusual activity is identified. When a suspicious activity is detected EDD should be considered.

EDD goes further than obtaining CDD. It involves considering whether additional identification information needs to be obtained on the customer, considering whether additional verification of identity is required, taking reasonable measures to establish source of wealth (in addition to source of funds) of the customer and beneficial owner and considering what ongoing monitoring of this information should be undertaken. It is important that licenceholders document details of the additional measures taken and provide justification for any decisions made.

The IOMFSA understands that the cost of operating higher risk relationships can be significant; however, the requirements for EDD and more frequent monitoring is a necessary preventative measure and is an international standard that is not unique to the Isle of Man. These costs, when balanced against income derived from such relationships can be one factor that may be leading to some financial institutions / groups (particularly banks) turning away business or closing existing relationships. The issue of banks' de-risking is recognised internationally and continues to be subject to review and discussion. It should however be noted that other factors that are not related solely to AML/CFT also play a part in banks' decisions.

10. Will any further guidance be provided in relation to customer risk assessments?

It is envisaged the AML/CFT Handbook will be amended in due course to reflect the findings of the National Risk Assessment, this may therefore impact on the "Customer Risk Assessment" section of the AML/CFT Handbook. Notification would be given to regulated entities at the time of any such update.