ML/FT Risk Assessments

Jonathan Phyall
Legal Affairs Section

The Revised Implementing Procedures Part I – 18 October 2019

Assessing Exposure to ML/FT Risk

- An assessment to be carried out at two levels:

  - At the business level so as to identify and assess the ML/FT risks the Subject Person is exposed to due to the activities or business it carries out (**"Business Risk Assessment"**); and

  - At the customer level whenever entering into a business relationship or carrying out an occasional transaction to identify and assess the specific ML/FT risks arising from the business relationship or occasional transaction (**"the Customer Risk Assessment"**).

- In both instances lead to a determination of what measures, policies, controls and procedures are to be adopted and implemented to effectively mitigate the resulting ML/FT risks, including any necessary resources.

The Business Risk Assessment (1)

- What are the requirements under the PMLFTR for the Business Risk Assessment? It must:

  a. Take into account the main risks including those relating to customers, countries or geographical areas, products, services, transactions and delivery channels;

  b. Be proportionate to the Subject Person's nature and size of its business; and

  c. Be regularly reviewed and kept up-to-date.

The Business Risk Assessment (2)

Taking Account of Risks (A)

- The Business Risk Assessment has to document what are the subject person's inherent risks. It is therefore necessary to:
  - Identify and set out the risks referred to in the PMLFTR – as a minimum customer risk, geographical risk, delivery channel(s) risk and the product, service and/or transaction risk.
  - Consider other risk factors – reliance, outsourcing etc.
  - What is the inherent risk, i.e. likelihood and impact of risk materialising itself.
- No single methodology being recommended as long as it can be shown to be effective.

The Business Risk Assessment (3)

Taking Account of Risks (B)

Table 1 – Likelihood scale

Likelihood Scale Frequency	Likelihood of ML/FT Risk
4 – Extreme	Can occur several times a year – very high chance
3 – High	Can occur a few times a year – reasonable chance
2 – Medium	Can occur once a year – small chance
1 – Low	Can occur less than once a year – very unlikely

Table 2 – Impact scale

Consequence	Impact of ML/FT Risk
4 – Extreme	Severe loss or damage, heavy supervisory action – long-term effect
3 – High	Large loss or damage, supervisory action – medium-term effect
2 – Medium	Limited loss or damage, minor supervisory action – short-term effect
1 – Low	Negligible loss or damage, no supervisory action – no effect

The Business Risk Assessment (4)

Taking Account of Risks (C)

Table 3 – Inherent Risk

IMPACT / LIKELIHOOD	1	2	3	4
1	Low Risk	Low Risk	Moderate Risk	High Risk
2	Low Risk	Low Risk	Moderate Risk	Extreme Risk
3	Moderate Risk	Moderate Risk	High Risk	Extreme Risk
4	High Risk	High Risk	Extreme Risk	Extreme Risk

The Business Risk Assessment (5)

Taking Account of Risks (D)

- Risk factors have to considered from the qualitative as well as quantitative aspect.
- Examples:
  - Customer risk – Companies undertaking activities known to be exposed to corruption, bribery etc. But how many such customers? What volume of business do they represent?
  - Geographical risk – Countries with high levels of criminality/corruption. But how many customers from these areas? How many transactions to/from these areas?

The Business Risk Assessment (6)

Taking Account of Risks (E)

- Linked to the question of risks is the question of effectiveness of the mitigating measures adopted. This should equally result from the Business Risk Assessment.

Level of Mitigation	Description of Effectiveness
4 – Strong	There are measures in place to control risk that are fully operational and fully effective
3 – Effective	Risk is managed adequately but could be improved in certain parts – mitigating measures work adequately and are effective
2 – Ineffective	Risk is not managed adequately, substantial improvement necessary but has some effect
1 – Non-Existent	No controls or controls are ineffective

The Business Risk Assessment (7)

Proportionate to the Nature and Size of its Business

- Consider the nature, size and complexity of:
  - One's systems and structures (e.g. network of branches and agents, number of employees, interaction channels etc.); and
  - One's activities (e.g. diversified customer base, complex transactions, multiple products/services, international outreach etc.).
- Not a question of the document's length but of its relevance.

The Business Risk Assessment (8)

Regularly Reviewed and Kept Up-to-Date

- To be undertaken prior to the commencement of operations on the basis of the expectations of the Subject Person.

- Reviews and, if needed, updates are necessary as risk is not static.

- When?
  - New threats and/or vulnerabilities are identified
  - Changes to business model/structure/activities
    (Planned changes – new markets, new technologies, new products/services - not to take effect prior to review of the Business Risk Assessment)
  - Changes to the external environment
  - Unless otherwise provided, on an annual basis

The Business Risk Assessment (9)

Regularly Reviewed and Kept Up-to-Date

- In the event of an update of the Business Risk Assessment, one has to:

  ➢ Review the mitigating measures available to ensure that they are sufficient to address the new risks or otherwise have to strengthen the same;

  ➢ Review any effected Customer Risk Assessment to ensure that it reflects the new level of risk identified in the Business Risk Assessment.

The Business Risk Assessment (10)

- Is there a need for the Business Risk Assessment to be produced in-house?

- No, it can be produced internally but it can also be produced:

  - With the assistance of external consultants;
  - Through sectoral/industry representative bodies;
  - At the group level.

- **However**, responsibility for the Business Risk Assessment rests **only** with the subject person.

- Have to ensure that it is relevant and covers all areas of risks to which one is exposed.

The Business Risk Assessment (11)

- Business Risk Assessment, including methodology used, has to be documented.

- Outcome of the review process and any updates have to also be documented.

- Approved and adopted by the subject person, i.e. by the Board of Directors, equivalent function or by the individual carrying out the relevant activity or the relevant financial business.

Is an exemption from the Business Risk Assessment possible?

Yes, but it can only be granted by the FIAU to a whole sector if it considered that the risk is clear and understood – not for individual subject persons.

The Business Risk Assessment (12)

- There are a number of information sources that can be considered for the Business Risk Assessment. As a minimum have to take into consideration:

  - **Supranational Risk Assessment**
  - **National Risk Assessment**

- **Taking into account the NRA Results**

  - **Domestic Tax Evasion** – A subject person servicing domestic customers faces a significant risk of being used to launder the proceeds of tax evasion

  - **Identify and assess the corresponding risk**
    - A Subject Person should demonstrate that it assessed the potential risk and exposure it faces in relation to ML resulting from tax evasion
    - What type of **customers** are likely to pose such a risk?
    - What type of **products / services** are more likely to be misused for such a purpose?

The Business Risk Assessment (13)

➢ **Taking into account the NRA Results**

- **Organised crime groups and links with high-risk neighbouring countries** – The Maltese financial system faces a significant risk of being exploited by international crime groups especially from neighbouring countries.

- **Identify and assess the corresponding risk**
  - A Subject Person should demonstrate that it assessed the potential risk of being misused for such purpose
  - Does the **geographical risk assessment** take this in consideration?

- **As the first line of defence** - Subject person has to be aware of what the country's ML/FT risks are and be able to effectively deter them from materialising and/or detect them.

The Business Risk Assessment (14)

- **Sectorial Vulnerability – TCSPs**
  - Unnecessary complex / multi-tiered structures – **Product / Service Risk**
  - Servicing of high-net worth individuals – **Customer Risk**
  - Non-resident clients (including exposure to high-risk jurisdictions) – **Customer Risk**
  - Non-face to face service provision & Use of Intermediaries – **Interface Risk**

- **Sectorial Vulnerability – Take-aways**
  - Are complex and multi-tiered structures considered as high risk factors in your product / service assessment?
  - Do you treate foreign nationals/ residents with more caution and where necessary subjecting them to EDD?
  - Do you take into consideration the use of intermediaries as a risk factor?

The Business Risk Assessment (15)

- **Sectorial Vulnerability – Banks**
  - Inherently exposed to risk due to type of products offered – **Product / Service Risk**
    - *Non-retail deposits, Correspondent Accounts, Wire Transfers and Wealth Management*
  - Proportion of high-risk clients (e.g. Non-EU residents, PEPs) – **Customer Risk**
  - Risk due to non-face-to-face clients introduced through intermediaries (e.g. CSPs, Trustees) – **Interface Risk**

- **Sectorial Vulnerability – Take-aways**
  - Are the services / products mentioned in the NRA as products posing a high risk of ML/FT being duly considered in your BRAs and subject to effective AML/CFT controls?
  - PEPs & Non-Residents – Are these treated with more caution and scrutiny?
  - Intermediaries and Introducers of Business – Are these considered in your BRAs as high risk types of business, and subject to commensurate scrutiny?

Customer Risk Assessment Procedures (1)

- The Customer Risk Assessment is to:
  - Be carried out prior to entering into a business relationship and/or carrying out an occasional transaction;
  - Be revised, and if necessary updated, whenever there occur triggering events (e.g.: changes in usual transactional patters, requests for new services/products etc.).
- The Customer Risk Assessment is a 'continuous' process – at on-boarding stage it may be too early to identify exactly the level of risk presented by a customer.
- To be carried out by the individual subject person.

Customer Risk Assessment Procedures (2)

- Up to the subject person to adopt the most appropriate methodology to carry out the customer risk assessment.

- However:

  - It must be understood by the subject person;
  - It needs to reflect the conclusions of the Business Risk Assessment;
  - It has to be adopted and approved of by the Board of Directors or equivalent function (where applicable); and
  - It has to be documented.

- Outcome allow an understanding of the overall risk, whether it falls within the risk appetite of the subject person, and what measures to adopt.

Customer Risk Assessment Procedures (3)

- What factors are to be considered in carrying out the Customer Risk Assessment? Same four categories as for the Business Risk Assessment.

- The relevance of a risk factor will not be always the same for all business relationships or occasional transactions.

- However, the relevance may vary due to aspects like the purpose for establishing the business relationship, the level of assets involved or size of transactions involved etc.

- Important that there is sufficient leeway when determining the weight to be assigned to each risk factor to consider how this may vary on the basis of the specific case.

Customer Risk Assessment Procedures (4)

Example:

Country 'A' is known to be rife with corruption
Country 'B' is known to harbour terrorist organisations

Customer asks to remit small amounts to recipients in both Country 'A' and Country 'B'

In both instances the geographical risk would be high but it would be higher in respect of remittances to Country 'B' – Geographical risk should carry a heavier weighing in the case of remittances to Country 'B'.

Why? Small amounts + terrorist organisations = higher risk of terrorist financing

Customer Risk Assessment Procedures (5)

- Important that:
  - Weighing is not influenced by any one factor
  - Monetary considerations do not influence the risk rating
  - The provisions of law on situations requiring the application of EDD are not overridden
  - Weighing does not lead to a situation where no relationship or occasional transaction is rated as high risk

Jonathan Phyall
jonathan.phyall@fiumalta.org

65C, Tower Street, Birkirkara BKR 4012, Malta

T. (+356) 21 231 333 F. (+356) 21 231 090 E. info@fiumalta.org W. fiumalta.org