The Risk Based Approach

Jonathan Phyall
Legal & International Relations Section

Consultation Exercise
Revision of the FIAU Implementing Procedures - Part I
18/19 December 2018
General Overview

• Introduction to the Risk Based Approach
  - Fundamentals
  - The Legal Framework

• The Business Risk Assessment

• Measures, Policies, Controls and Procedures

• Customer Risk Assessment Procedures

• Level of Customer Due Diligence

• Information Resources
The Fundamentals (1)

- Risk is composed of two elements:
  - **Likelihood** that something will go wrong; and
  - **Impact** this will have on who incurs the risk (financial, reputational etc.)

- It is the **inherent risk** that has to be considered and not the **residual risk**, i.e. the risk prior to the application of any mitigating measures.
The Fundamentals (2)

• To determine likelihood one has to first determine to which risk factors one is exposed to, i.e. one has to determine from where risk can arise.

• Risk factors can be sub-divided into:

  - **Threats** – the external elements giving rise to risk (e.g. customers)
  - **Vulnerabilities** – the internal elements giving rise to risk (e.g. product characteristics)

• Likelihood – the possibility that a threat will exploit one or more of your vulnerabilities over a period of time leading to the materialisation of risk.
The Fundamentals (3)

• Impact – Given the likelihood of risk materialising itself, what consequences will one suffer?

  ➢ Financial – Loss of business, earnings etc.
  ➢ Regulatory – Supervisor or regulatory authority may take action and the nature of the action taken.
  ➢ Reputational – Loss of trust by other market participants, existing or prospective customers.
The Fundamentals (4)

- To effectively address risk, stronger mitigating action is required where the likelihood of something going wrong and the impact this would have is higher than in other situations.

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Impact</th>
<th>Mitigating Action Required</th>
<th>(Desired) Residual Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Great</td>
<td>Strong</td>
<td>Minimal</td>
</tr>
<tr>
<td>Low</td>
<td>Minimal</td>
<td>Weak</td>
<td>Minimal</td>
</tr>
</tbody>
</table>

- **Residual risk** will indicate if the situation falls within one’s **risk appetite**.
The Fundamentals (5)

- Risk is not something removed from our daily lives ...

What to do when it rains?
The Fundamentals (6)

- The likelihood of being late or catching a cold ...
The Fundamentals (7)

- The impact ...
The Fundamentals (9)

- Your mitigating measures ...
By adopting a risk-based approach, competent authorities and financial institutions are able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate to the risks identified ... The principle is that resources should be directed in accordance with priorities so that the greatest risks receive the highest attention.

The Legal Framework (1)

- The Prevention of Money Laundering and Funding of Terrorism Regulations 2008 already included elements of the risk-based approach:
  - Requirement to carry out a customer risk assessment to determine if a business relationship/occasional transaction presented a high risk of ML/FT
  - Requirement to apply Simplified Customer Due Diligence (“SDD”) only once the subject person determines that the risk of ML/FT is actually low
  - The option to apply a risk-based approach and potentially be able to apply SDD even in situations which were not statutorily considered as low risk
The Legal Framework (2)

4.1 Mandatory risk procedures

Subject persons are required to have in place procedures to manage the ML/FT risks posed by their customers,\(^{47}\) products and services. This requirement is found under Regulation 4(1)(c) which stipulates that subject persons are to establish procedures on, *inter alia*, **risk assessment** and **risk management** that are adequate and appropriate to prevent the carrying out of operations that may be related to ML/FT.
The Legal Framework (3)

• Directive (EU) 2015/849 widened the application of the risk-based approach:

The risk of money laundering and terrorist financing is not the same in every case. Accordingly, a holistic, risk-based approach should be used. The risk-based approach is not an unduly permissive option for Member States and obliged entities. It involves the use of evidence-based decision-making in order to target the risks of money laundering and terrorist financing facing the Union and those operating within it more effectively.

Directive (EU) 2015/849 (Recital 22)

• This has been reflected in the Prevention of Money Laundering and Funding of Terrorism Regulations 2017 (“PMLFTR 2017”)
The Legal Framework (4)

• Under the PMLFTR 2017 subject persons have to:

  ➢ Carry out a business risk assessment [Regulation 5(1)]

  ➢ Have in place risk management procedures, including procedures for assessing the risk of ML/FT presented by a given business relationship or an occasional transaction [Regulation 5(5)(a)(ii)]

  ➢ Determine themselves any additional situations in which to apply Enhanced Customer Due Diligence ("EDD") (Regulation 11(1)(b)]

  ➢ Determine themselves the situations in which to apply SDD [Regulation 10(1)(b)]
The Business Risk Assessment (1)

• Why is there a requirement to carry out a Business Risk Assessment?

1. What is the purpose of a risk assessment?

The key purpose of a money laundering risk assessment is to drive improvements in financial crime risk management through identifying the general and specific money laundering risks a FI is facing, determining how these risks are mitigated by a firm’s AML programme controls and establishing the residual risk that remains for the FI.


• The Business Risk Assessment is a study to determine the inherent risks you are exposed to and where should action be taken and resources invested.
The Business Risk Assessment (2)

- What are the requirements under the PMLFTR 2017 for the Business Risk Assessment?

  1. Takes into account risk factors including those relating to customers, countries or geographical areas, products, services, transactions and delivery channels;

  2. Proportionate to the nature and size of its business; and

  3. Is regularly reviewed and kept up-to-date.
The Business Risk Assessment (3)

*Takes Account of Risk Factors (A)*

- The Business Risk Assessment has to document what are the subject person’s inherent risks. It is therefore necessary to:
  - Identify the risk factors 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 (4)

* Takes Account of Risk Factors (B) *

<table>
<thead>
<tr>
<th>Table 1 – Likelihood scale</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Likelihood Scale Frequency</strong></td>
</tr>
<tr>
<td>4 - Extreme</td>
</tr>
<tr>
<td>3 - High</td>
</tr>
<tr>
<td>2 - Medium</td>
</tr>
<tr>
<td>1 - Low</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 2 – Impact scale</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Consequence</strong></td>
</tr>
<tr>
<td>4 - Extreme</td>
</tr>
<tr>
<td>3 - High</td>
</tr>
<tr>
<td>2 - Medium</td>
</tr>
<tr>
<td>1 - Low</td>
</tr>
</tbody>
</table>
## The Business Risk Assessment (5)

*Takes Account of Risk Factors (C)*

### Table 3 – Inherent Risk

<table>
<thead>
<tr>
<th>IMPACT</th>
<th>LIKELIHOOD</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Low Risk</td>
<td>Low Risk</td>
<td>Moderate Risk</td>
<td>High Risk</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Low Risk</td>
<td>Low Risk</td>
<td>Moderate Risk</td>
<td>Extreme Risk</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Moderate Risk</td>
<td>Moderate Risk</td>
<td>High Risk</td>
<td>Extreme Risk</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>High Risk</td>
<td>High Risk</td>
<td>Extreme Risk</td>
<td>Extreme Risk</td>
<td></td>
</tr>
</tbody>
</table>
The Business Risk Assessment (6)

*Takes Account of Risk Factors (D)*

- Risk factors have to be 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 (7)
The Business Risk Assessment (8)

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 (9)

Regularly Reviewed and Kept Up-to-Date

- To be undertaken prior to the commencement of operations or, for existing activities, as soon as possible.

- 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 (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.
Measures, Policies, Controls and Procedures (1)

- The PMLFTR 2017 require a subject person to have in place and implement:
  - Measures, policies, controls and procedures;
  - Proportionate to the nature and size of the subject person’s business; and
  - Address the risks identified as a result of the Business Risk Assessment.
Measures, Policies, Controls and Procedures

• Customer due diligence measures, record keeping and reporting procedures.

• Risk management measures including customer acceptance policies, customer risk assessment procedures, internal control, compliance management, communications, employee screening policies and procedures.
Proportionate to the Nature and Size of the Business
Address the Risks Identified through the Business Risk Assessment

• A self-employed subject person who interacts with customers on a face-to-face basis and offers only a limited spectrum of services to domestic customer.

• A subject person forming part of a multinational group of companies interacting with customers through various channels and offering products to customers located in or with links with various jurisdictions.
Measures, Policies, Controls and Procedures (4)

Rating Effectiveness

**Table 4 – Effectiveness**

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

- Does the residual risk fall within your risk appetite?
  - Yes – No further action
  - No – Additional measures required or no longer pursue business
Measures, Policies, Controls and Procedures (5)

Effectiveness – Uniform Application and Revision

• Measures, policies, controls and procedures mitigate risk only if they are applied in a proper and uniform manner.

• Revision of measures, policies, controls and procedures whenever new risks are identified or changes to business are planned.

Hence the need for:

• Informing officers and employees about the measures, policies, controls and procedures, and train them on how to apply them.

• Have regular audits (internal or external) and compliance function.
Measures, Policies, Controls and Procedures (6)

*The Customer Acceptance Policy*

- The main policy setting out the kind of customers that a subject person is ready to service and offer its products to.

- Explains the measures, procedures and controls that are to be applied to different categories of customers, especially in which circumstances it may be possible to apply SDD and in which EDD is required.

- Provide examples of who falls within given categories, including risk indicators that may be more generic.

- And don’t forget to cover Politically Exposed Persons ...
Measures, Policies, Controls and Procedures (7)

_Last Famous Words..._

• Controls, policies, measures and procedures, including any revision and update of the same, have to be documented.

• Consultants can assist subject persons but ultimate responsibility rests with the subject person concerned.

• Have them approved by your Board of Directors or equivalent body.
Customer Risk Assessment Procedures (1)

• Process to determine the risk presented by a given business relationship to be entered into or by an occasional transaction to be carried out.

• On the basis of risk factors and risk level identified can apply the measures provided for in the Customer Acceptance Policy.

• To consider amongst others the risk factors identified through the Business Risk Assessment.
Customer Risk Assessment Procedures (2)

• 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 patterns, 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 (3)

- 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.
Customer Risk Assessment Procedures (4)

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

• **Customer Risk**

  - Customer’s Business or Professional Activity  
    (usually already identified at the stage of the Business Risk Assessment)

  - Customer’s Reputation  
    (not limited to convictions - reliable public information resources)

  - Customer’s Nature and Behaviour  
    (reluctance to provide information, sudden changes to control structure etc.)
Customer Risk Assessment Procedures (5)

- **Geographical Risk**
  
  (Depends on the nature of the connection – place of birth on its own need not translate in a determination of high or low risk)

- **Delivery Channel Risk**

- **Product/Service/Transaction Risk**
  
  (volume of transactions and amount per transaction)
Customer Risk Assessment Procedures (6)

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

- 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 (7)

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 (8)

- 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
Level of Customer Due Diligence (1)

- Through the Customer Risk Assessment a subject person identifies:
  - The specific risk factors that may give rise to a high risk of ML/FT; and
  - The overall risk level presented by the business relationship or occasional transaction.

- Calibrate accordingly the level of Customer Due Diligence to be applied:
  - Timing when Customer Due Diligence is carried out
  - Quality and Quantity of information/documentation to be collected
  - Frequency and/or intensity of on-going monitoring
  - Frequency of document/information/data updates
Level of Customer Due Diligence (2)

• Overall risk level is low -------- > apply SDD

• SDD is not an exemption from Customer Due Diligence but:

  (i) as a minimum identify the customer and level of on-going monitoring to ensure still low risk; and

  (ii) vary the extent of the other Customer Due Diligence measures or delay them till the happening of pre-determined events.
Level of Customer Due Diligence (3)

- Annex II to Directive (EU) 2015/849 lists a number of potentially low risk factors which can lead to the application of SDD

Example: Listed Public Company

On-Boarding: Company active in the mining industry and requires the creation of complex structures to channel funds to undisclosed recipients

On-Going Monitoring:
(a) Company is delisted
(b) Company is fined for breach of disclosure requirements

Can it be said that it is low risk?
Level of Customer Due Diligence (4)

Petrobras hit with $853m corruption fine

27 September 2018

Novartis settles charges alleging bribery in China - SEC

March 23 (Reuters) - Drugmaker Novartis AG agreed on Wednesday to pay more than $25 million to the U.S. government to settle civil charges that it bribed healthcare professionals in China to boost sales there, the U.S. Securities and Exchange Commission said.

The SEC said violations of a U.S. law barring bribery of foreign officials occurred from 2009 to 2013. Novartis settled the charges without admitting or denying them, the SEC said. (Reporting by Jonathan Stempel and David Ingram in New York; Editing by Jonathan Oatis)

Our Standards: The Thomson Reuters Trust Principles.
Level of Customer Due Diligence (5)

- Notwithstanding that the risk assessment may indicate a low level of risk, SDD cannot be applied where:
  - There is a suspicion of ML/FT;
  - There is a legal obligation to apply EDD measures; or
  - Any previous determination by authorities that a product/service is low risk is revoked
Level of Customer Due Diligence (6)

• Overall risk level is high -------- > apply EDD

• Enhanced Due Diligence measures must address the risk factors actually giving rise to risk.

Example:  If risk is originating from the activity carried out by the customer, the collection of additional identification document cannot be considered as an effective mitigating measure.

Collecting additional information on the nature of his activities, a higher level of on-going monitoring etc. may be more appropriate.
Level of Customer Due Diligence (7)

- In situations which the law considers high risk and it sets out the measures to be applied, there is still room to calibrate the measures to be applied to the circumstances at hand.

**Example:**
- The child of a PEP opens an account to receive his/her university stipend.
- A foreign PEP applies to open an account with a local institution even though he may be only sporadically present in Malta, with an expected high level of activity.

What level of source of wealth and source of funds information/documentation is required?
Information Resources (1)

- The law makes express reference to the Supranational Risk Assessment and to the National Risk Assessment.

- The European Supervisory Authorities’ Risk Factor Guidelines are especially important for anyone carrying out relevant financial business:
  - Emphasis on the customer risk assessment aspect;
  - Provide guidance as to specific risk factors and the level of risk associated therewith for particular services/products;
  - Set out mitigating measures that can be taken or how to apply Simplified Due Diligence

- Justifiable reasons for diverging from the same.

- May be useful event to anyone carrying out relevant activities.
Information Resources (2)

- Other documents that can be of assistance include:
  - Mutual Evaluation Reports carried out by the FATF or FSRBs like Moneyval
  - Typologies reports produced by the FATF, FSRBs like Moneyval, domestic and foreign authorities
  - Guidance, reports and opinions issued by the European Supervisory Authorities, the European Central Bank, the International Monetary Funds, the Bank for International Settlements etc.
  - Reports and information from other reputable bodies or sources
Feedback Already Received

- **Presentation of Risk Factors in Section 3.2 is not very helpful**

  There is a need to better distinguish between risk factors that are relevant for the carrying out of the Business Risk Assessment and those relevant for the Customer Risk Assessment.

- **Table 5 and Table 6 need to be revised**

  These are examples and do not necessarily reflect the FIAU’s point of view. However, the retention of the said tables has to be considered further and may have to be revised.

- **Better streamlining of the terminology used throughout the revised text**
THANK YOU

QUESTIONS?