Applying a Risk-Based Approach ("RBA")

Relevant Persons are required to apply an approach to their Anti-Money Laundering, Counter-Terrorist Financing compliance (collectively referred to as AML compliance) which is proportionate to the risks to which the Relevant Person is exposed to as a result of the nature of its business, customers, products, services and any other matter which may be relevant.

The general principle is that where there are higher risks of money laundering taking place, enhanced measures to manage and mitigate those risks should be implemented. Correspondingly when the risks are lower, simplified measures are permitted.

Adopting the RBA discourages a "tick box" attitude to AML compliance and instead emphasises that there should be a clear and reasonable rationale for the measures taken by Relevant Person to manage and mitigate the AML risks which it faces. The process of applying the RBA will vary from Relevant Person to Relevant Person and it is important for a Relevant Person to tailor its processes to its individual risks.

It is for these reasons that the AML Module does not prescribe, beyond what is contained in the AML Module, how a Relevant Person should implement its risk-based approach. However, it is important to note that Chapter 4 of the module sets out the standard for risk-based assessments and applies to all decisions made by a Relevant Person in which a risk-based assessment is required. The four elements of any risk-based assessment are that they should be:

- Objective and proportionate to the risks;
- based on reasonable grounds;
- properly documented;
- reviewed and updated at appropriate intervals

The DFSA provides interpretative Guidance throughout the AML Module. The information contained in these webpages is designed to complement the Rulebook Guidance by providing useful resources and practical examples for Relevant Persons to consider when developing and implementing a RBA.

Relevant Resources

Financial Action Task Force (FATF)

In developing the AML Rulebook the DFSA has had regard and been guided by the FATF and in particular its International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, also known as the FATF Recommendations. The AML Module is substantively in compliance with the FATF standards and is, in some limited cases, super-equivalent. A Relevant Person may find it useful to consider the contents of the FATF Recommendations in complying with their obligations under the AML Module.

The FATF Recommendations can be found using the following link:

http://www.fatf-gafi.org/topics/fatfrecommendations/documents/internationalstandardsoncombatingmoneylaunderingandthefinancingofterrorismproliferation-thefatfrecommendations.html

In addition, FATF has established an Electronic Advisory Group ("EAG") which has produced guidance to support the development of a common understanding of what the RBA involves, outline the high level principles involved in the RBA, and to share good practice in the design and implementation of an effective RBA. The first FATF EAG guidance published can be found using the following link:

http://www.fatf-gafi.org/media/fatf/documents/reports/RBA%20ML%20and%20TF.pdf

FATF has also published a number of sector-specific Guidance Papers which may be applicable to Relevant Persons including:

Trust and Company Service Providers:

http://www.fatf-gafi.org/media/fatf/documents/reports/RBA%20for%20TCSPs.pdf

Real Estate Agents:
http://www.fatf-gafi.org/media/fatf/documents/reports/RBA%20Guidance%20for%20Real%20Estate%20Agents.pdf

Dealers in Precious Metals and Stones:
http://www.fatf-gafi.org/media/fatf/documents/reports/RBA%20for%20Dealers%20in%20Precious%20Metal%20and%20Stones.pdf

Accountants:
http://www.fatf-gafi.org/media/fatf/documents/reports/RBA%20for%20accountants.pdf

Legal Professionals:
http://www.fatf-gafi.org/media/fatf/documents/reports/RBA%20Legal%20professions.pdf

Life Insurance Sector:
http://www.fatf-gafi.org/media/fatf/documents/reports/RBA%20Guidance%20for%20Life%20Insurance%20Sector.pdf

Other information which can be found on FATF's website includes:

- Mutual Evaluation Reports; http://www.fatf-gafi.org/topics/mutualevaluations/
- Typology Reports; http://www.fatf-gafi.org/topics/methodsandtrends/ and
- Guidance and Best Practice Reports. http://www.fatf-gafi.org/documents/guidance/

Good and Bad Practices

In June 2011 the Financial Services Authority ("FSA")[1] published a report entitled "*Banks' management of high money laundering risk situations",* examining how banks

[1] Now the Financial Conduct Authority ("FCA").

operating in the UK were managing money laundering risks in high risk situations. The report provides some very good examples of good and bad practices and can be accessed using the following link:

http://www.fsa.gov.uk/pubs/other/aml_final_report.pdf

The table below provides examples of good and bad practices relating to the RBA some of which are found in the above FSA report.

Good Practices	Bad Practices
The RBA is supported by objective and credible resources such as international or industry standard-setters e,g FATF typology reports.	A Relevant Person's RBA methodology is arbitrary and without justification, and is based on the personal views of a small number of individuals within the Relevant Person.
The Relevant Person documents the rationale for its decisions when adopting the RBA.	The Relevant Person's RBA and the decisions made which flow from its systems and controls and RBA policies are not supported by sufficient or any documentation. Lack of documentation hinders contribution from others within the Relevant Person and can make any meaningful on-going monitoring or review of the RBA difficult.
Risk assessment policies which reflect the Relevant Person's risk assessment procedures and risk appetite.	Risk assessment is a one-off exercise. It may have been fit for purpose at the time but fails to keep up-to-date with changes both within the Relevant Person and its external environment.
Clear understanding and awareness of risk assessment policies, procedures, systems and controls among relevant staff.	Efforts to understand risk are token and not communicated to relevant employees and risk assessments are a tick box process.
Risk assessment is a continuous process based on the best information available from internal and external sources.	The Relevant Person targets money laundering practices that affect the bottom line (eg money laundering against the Relevant Person) but neglects those relating to third parties (eg money laundering against customers).
The Relevant Person uses robust risk assessment systems and controls appropriate to the nature, scale and complexities of the Person's business.	An inappropriate risk classification system makes it almost impossible for a relationship to be assigned a 'high risk' classification, whether deliberately or inadvertently. In worse case scenarios the classification system is engineered to fit the compliance resources of the Relevant Person instead of the risk level helping to determining the level compliance resources required.
The Relevant Person has identified good sources of information on money laundering risks, such as FATF mutual evaluations and typology reports, press reports, court	A DFSA branch or subsidiary relies on group risk assessments without assessing their compliance with DFSA AML requirements.

judgements, reports by non-governmental organisations and commercial due diligence providers.	
Quality assurance work to ensure risk assessment policies, procedures, systems and controls are working effectively in practice.	Higher risk countries are assigned low risk scores to avoid enhanced due diligence measures.

Assessing Business Risk

Chapter 5 of the AML Module requires a Relevant Person *to identify and assess money laundering risk its business is exposed to taking into consideration the nature, size and complexity of its activities.*

Factors to be considered when undertaking the assessment of business risk include, but should not be limited to:

- Type of customers and their activities;
- Countries or geographic areas in which a Relevant Person does business;
- Products, services and activity profiles;
- Distribution channels and business partners;
- The complexity and volume of transactions;
- The development of new products and new business practices, including new delivery mechanisms, channels and partners; and
- the use of new or developing technologies for both new and pre-existing products.

The process of identifying components of business risk involves a level of introspection and deliberation drawing on the collective experience within the Relevant Person, from senior management to operational staff.

Relevant Resources

In assessing and identifying business risks Relevant Persons may be assisted by external resources and other publicly available information such as the FATF publications referenced above.

Another useful source of information can be obtained from industry bodies such as the UK's Joint Money Laundering Steering Group, which has published a significant amount of general and sector-specific guidance on AML.

http://www.jmlsg.org.uk/

The Wolfsberg Group[2] has also published a number of papers on topics such as Correspondent Banking, Corruption, Stored Credit and Trade Finance.

http://www.wolfsberg-principles.com/index.html

Once done, the business risk assessment may remain relatively static and would need only change as a result of a change or shift in Relevant Person's activities. However, the responsibility to regularly re-assess business risk is required under the AML Module.

Good and Bad Practices

Good Practices	Bad Practices
RBA and business risk assessment is conducted with appropriate input and buy-in from operational areas of the Relevant Person where risk can be considered from a compliance and commercial perspective.	Business risk assessment is conducted in isolation within the Relevant Person with little or no input from operational areas, leading to a lack of understanding of the risks identified.
Risk associated with jurisdictions in which the Relevant Person does business has been assessed on objective and reasonable grounds, utilising information from reputable sources.	Risks of jurisdictions are under estimated based on irrelevant factors such as presence of a branch office or personal experiences of a country.
Business risk assessment is sufficiently detailed to identify the different risks poses by different business lines within the Relevant Person.	The business risk assessment is conducted at too high a level resulting in a generalised risk profile.
The findings of the business risk assessment are used to develop the Relevant Person's policies, procedures, systems and controls. Allowing the allocation of resources and ensure greater scrutiny for higher risk activities, while reducing the burden for lower risk activities.	A generalised business risk assessment which leads to insufficient consideration of higher risk activities and unwarranted or excessive attention being given to lower risk activities.
The Relevant Person considers money laundering / terrorist financing risk when designing new products and services.	Money laundering risk assessments are unduly influenced by the potential profitability of new or existing relationships.

Assessing Customer Risk

Having determined its business AML risk, chapter 6 of the AML Module requires a Relevant Person to assess the AML Risk posed by its customers. The factors to be considered when undertaking an assessment of customer risk include, but should not be limited to:

[2] The Wolfsberg Group is an association of eleven global banks, which aims to develop financial services industry standards, and related products, for Know Your Customer, Anti-Money Laundering and Counter Terrorist Financing policies.

- identifying the customer and any beneficial owner;
- obtain information on the purpose and intended nature of the business relationship;
- the nature of the customer, its ownership and control structure;
- the nature of the customer business relationship with the Relevant Person;
- the customers country of origin, residence, nationality, place or incorporation or place of business;
- the relevant product service or transaction;
- business risk assessment under Chapter 5 of AML Module.

Relevant Resources

Publicly available information and resources that Relevant Persons may wish to utilise when it is designing and implementing its customer risk assessment include:

- FATF Information on High Risk and Non-Cooperative Jurisdictions:

http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/

- Transparency International: ("TI"). TI is a non-profit, non-governmental organisation dedicated to fighting corruption. TI publishes, amongst other information, a Corruption Perception Index which measures levels of perceived corruption around the world. Relevant Person will find this public resource useful in assessing the risks posed by different jurisdictions and this information can be used to inform your RBA.

http://www.transparency.org/

- Basel Institute on Governance: (BIG) is an independent not-for-profit competence centre specialised in corruption prevention and public governance, corporate governance and compliance, anti-money laundering, criminal law enforcement and the recovery of stolen assets. BIG also publishes the Basel AML Index country risk rankings which measures the risk of money laundering/ terrorist financing and other relevant aspects, such as financial standards and public transparency.

http://www.baselgovernance.org/big/

- The Basel AML Index aggregates third party data from sources such as FATF, World Bank and the Works Economic Forum to assess a country's overall money laundering risk.

http://index.baselgovernance.org/

Good and Bad Practices

Good Practices	Bad Practices
The customer risk assessment is based on appropriate risk considerations and the conclusions are properly documented.	The customer is considered lower risk based on the length of time the Relationship Manager at the Relevant Person has known the customer. While genuine indicators of low risk are ignored and not documented.
The Relevant Person identifies where there is a risk that a relationship manager might become too close to customers to identify and take an	Failing to properly risk assess customers until shortly before a regulatory inspection.

objective view of the money laundering risk. It manages that risk effectively.	
The Relevant Person determines beneficial owners based on relevant factors such as ownership, control, or on whose behalf the transaction is conducted or the benefit derived.	The Relevant Person relies solely on a percentage shareholding to determine beneficial ownership.
The Relevant Person rates a class of customers as low risk on the basis of predefined criteria but ensures on a regular basis that each customer continues to meet the relevant criteria or does not have another risk factor that raises the AML risks.	The Relevant Person uses a blanket approach to risk rating a customer class without proper justification and without random sampling for error.
The Relevant Person considers and places appropriate weight on the findings of the business risk assessment and its overall customer risk assessment to determine the appropriate level of Customer Due Diligence.	
The Relevant Person uses a clear, documented audit trail to show why customers are rated as high, medium or low risk.	The Relevant Person ignores or places insufficient weight on obvious AML risks or over emphasises low risk factors when undertaking risk assessments.

Frequently Asked Questions

1. Why is has the DFSA placed greater emphasis on the RBA?

A: The RBA is not a new concept and has always been part of the DFSA's AML framework. Under the AML Module a Relevant Person must ensure that it places greater emphasis on the identification and assessment of AML risk to ensure that resources are proportionately deployed.

2. How does using the RBA help me fight money laundering?

A: Increasing the emphasis on the RBA should focus a Relevant Person's time and resources on developing and administering a more proportionate and effective AML compliance culture. It should also help prevent a Relevant Person from adopting an approach to AML that is "tick box" e.g. by simply using detailed rules and guidance as a checklist rather than first identifying the AML risks associated with its business and customers and then adopting a response which is proportionate to the risks identified.

3. How does the RBA differ from Customer Due Diligence (CDD)?

A: *The RBA generally precedes CDD. It encourages a proper assessment of the AML risk presented by a person's business and customers and should inform and determine the level of CDD that should be undertaken for each customer.*

4. Why is a risk assessment required for both the business and customers?

A: *The AML risks that apply to a person's business and customer are different and should therefore be identified and analysed separately. The RBA requires that the risks facing a business and the risks posed by a customer be considered when determining the overall risk and the appropriate level of CDD to be performed. To consider the risks in isolation is likely to result in an inaccurate profile of the real risks. Understanding both types of risks is also important in allowing a Relevant Person to comply with its obligations under Federal Law No.4 of 2002 on AML. Failure to comply with Federal Law No.4 of 2002 can result in criminal sanctions.*

Further, unless a Relevant Person analyses and understands the AML risks to which its business is exposed, it cannot properly identify and mitigate AML risks. Once completed, a Relevant Person's assessment of its business risk should not vary materially in the short term and would only change significantly if a Relevant Person changes it business plan or strategic focus. By contrast, the customer risk assessment is customer specific and may vary significantly from customer to customer dependant on factors such as the jurisdiction of the customer or operates in and the value and frequency of a customer's transactions.

5. It is noted that the DFSA has provided some examples of the types of risks a Relevant Person should assess in relation to business and customers. Is this sufficient to meet the regulatory requirements?

A: *The types of risks and factors mentioned in the AML module and indeed as part of this FAQ are non-exhaustive and that there may be other factors that are relevant to a particular* Relevant *Person. The regulatory requirement is for a Relevant Person to utilise the RBA. How a Relevant Person chooses to implement this approach is a matter of judgement. However, Relevant Persons should ensure however that the decisions and considerations undertaken as part of their RBA are documented (see AML Section 14.4).*

6. We are only a small boutique operation with a small number of well-known customers. Are we still expected to carry out a risk assessment of the business and all our customers?

A: The AML Module does not provide any relief from applying the RBA based on the size of a Relevant Person or its number of customers. The only exemption from applying the risk based approach is found in Rule 4.2.2 of the AML Module which allows a Relevant Person to treat certain types of customer as 'automatically' having a lower risk.

A customer who is well known or has been a customer of Relevant Person for a lengthy period is not exempt from the customer risk assessment process. Often the history of the relationship will yield relevant facts that are very useful and may assist increasing or decreasing the risk. The Relevant Person should document these facts if they are to be relied upon.

7. We have a small number of customers which we have known for a considerable period of time. Do we need to do a risk assessment of these customers?

A: Yes. However, provided that any existing customer risk assessment is up-to-date and documented there may be no need to repeat the risk assessment. A Relevant

Person's existing in depth knowledge of its customers may help the Relevant Person to assess AML risks and may be a factor which reduces the perceived AML risk depending on the circumstances. However, Relevant Person should ensure that it documents the basis for its in depth knowledge.

8. What resources or lists should we use to decide what is a high risk jurisdiction?

A: There are a number of resources that Relevant Person's may use in determining the risks posed by different jurisdictions. These resources focus on different factors which can determine and influence whether a jurisdiction carries a higher risk than another. Such factors include a jurisdictions AML regulations, corruption, and transparency.

9. Our intention is for our MLRO to be responsible for carrying out a risk assessment of the business and customers, is the DFSA comfortable with this approach?

A: Chapter 3 of the AML Module places the responsibility for compliance with the AML Module on the Relevant Person's Governing Body or senior management. The pertinent question is therefore, whether the Governing Body or senior management is comfortable with the MLRO being responsible for carrying out the risk based assessment of the business and customers.

From a practical point of view the MLRO may be responsible for the carriage of the day to day steps in implementing the RBA but ultimate responsibility will rest with the Governing Body and senior management.

10. What role do you expect our Governing Body and senior management to play in the RBA?

A: Since a Relevant Person's Governing Body or senior management is ultimately responsible for a Relevant Person's compliance with the AML obligations, the DFSA would expect significant oversight and, where necessary, active involvement in a Relevant Person's RBA. Senior management are in a position to have a high level view across the Relevant Person's customer base and product offerings which gives them a unique and helpful insight.

However, it should be noted that the Governing Body or senior management's oversight should not restrict the MLRO's ability to act on his own authority.

11. If the Relevant Person has not yet signed on a person as a customer, but is liaising with a prospective customer does it still need to carry out a risk assessment of the prospective customer?

A: The DFSA guidance provides that a person becomes a customer where there is firm intention and commitment by each party to enter into a contractual or business relationship. At that point in time the person would be a customer and therefore the requirements of the AML Module must be met.

12. Do we need to carry out the business risk assessment prior to conducting client risk assessments?

A: There is no express requirement to carry out the assessment of business risks prior to the assessment of client risk, provided that both are completed and used to determine the level of CDD required for a customer. However, it is implied by the rules because the outcomes of the business risk assessment are required in order to undertake the customer risk assessment.

13. If the Relevant Person launches a new product or expects to provide a new service in the foreseeable future, does it need to carry out a new business risk assessment?

A: AML Rule 4.1.1(b) (vi) contemplates that Relevant Persons may develop new products and new business practices, and that these may be relevant factors to consider when assessing the business AML risk.

While it may not be necessary to carry out a new business risk assessment the current business risk assessment should be updated to take account of the new product or service.

14. When we carry out a risk assessment for the business and each customer, how much detail should we gather and does this need to be documented on file?

A: The assessments of business and customers should be sufficient to evidence the thought analysis undertaken by the Relevant Person. The assessments should be a narrative of the decision making process to both on board a customer and to determine the level of CDD which should be undertaken to mitigate any risks identified.

It is the Relevant Persons responsibility to determine how to implement its RBA. Documenting and recording the process undertaken is important, not only from a management information perspective, but also to evidence compliance with the AML Module.

15. Our current approach to AML is not risk based. Do we have a transitional period to conduct the necessary exercise to reassess all of our customers using the new approach?

A: There is no specific transitional period and the DFSA will deal with the implementation of the new provisions via its usual Supervisory channels. Any Relevant Person who has concerns with their ability to comply with the new provisions should contact the DFSA Relationship Manager. These issues will be dealt with on a case by case basis.

16. Should we have different RBA for Anti-Money Laundering and Counter-Terrorist Financing?

A: While the two subjects are separate and distinct, they overlap because terrorism is predicate offence for money laundering. They are also both criminal activities so the mechanisms used to detect and mitigate their associated risks are similar. Generally, the DFSA does not expect a separate RBA for the two. Rule 2.1.1 of the AML Module states that "references in this module to "money laundering" in lower case includes a reference to terrorist financing unless the context provides or implies otherwise".

17. Is the RBA about deciding whether the Relevant Person accepts a client or not? If so, does this mean a loss of potential customers? What if we carried out extra due diligence on the customer?

A: The decision of whether to accept a customer or not rests with the Relevant Person, which also bears the responsibility for the consequences of the decisions. An effective RBA should assist a Relevant Person in this decision making process through both identifying AML risks and providing the mechanisms to mitigate them. Enhanced CDD may assist in mitigating identified risks, but it is the Relevant Person which must make the decision as to whether a customer represents a risk that is beyond its risk appetite.

18. What format should our customer risk assessment take?

A: There is no prescribed format or template that a customer risk assessment should take, and Relevant Persons may use a format which suits them best. As mentioned previously, the RBA is not a "tick box" approach and each Relevant Person needs to consider its own individual circumstances.

Relevant Persons should ensure that their customer risk assessment and decision making process are adequately documented and recorded.

19. If we assess a customer as high risk what should we do next?

A: The outcome of the Relevant Person's customer risk assessment is the overall risk rating which will determine the level of CDD that should be undertaken.

Each customer should be assessed on a case by case basis and the ultimate decision should be adequately documented and recorded.

20. Who should be deemed a high risk customer?

A: Which customers should be assessed as high risk is ultimately up to the Relevant Person in accordance with its RBA. The DFSA provides guidance in Chapter 4 on the factors and situations that may indicate that a customer may pose a higher risk of money laundering and should be risk rated accordingly.

21. Does each department have to conduct separate risk assessment based on their respective operations?

A: The DFSA does not require that each department within a Relevant Person conduct separate risk assessments. It may be useful when designing its RBA to consult with subject matter experts within each department to ensure that the parameters of the RBA are being calibrated correctly.

22. Does the implementing of the new RBA prescribed by the DFSA apply only to new customers or must all existing customers be risk rated?

A: The AML Module applies to all of a Relevant Person's customers. Therefore, any deficiencies in the risk assessment or CDD for existing customers should be rectified as soon as identified and on an ongoing basis.