USING A RISK-BASED APPROACH TO COMBAT MONEY LAUNDERING AND TERRORIST FINANCING

IMPORTANCE OF A RISK-BASED APPROACH

All accountable institutions listed in Schedule 1 of the Financial Intelligence Centre Act, 2001 (Act 38 of 2001 (FIC Act) are required to apply a risk-based approach when establishing a business relationship and/or conducting a single transaction with a client.

This requirement emanates from a recommendation by the Financial Action Task Force (FATF), which sets international standards on combating money laundering and terrorist financing. The FATF’s Recommendations outline the standards and measures member countries need to adopt to advance the combating of money laundering and terrorist financing. As a member of the FATF, South Africa is required to adhere to the Recommendations and standards set by the organisation.

The FATF’s Recommendation 1 calls upon the identified entities of member countries’ to apply a risk-based approach when implementing controls to mitigate money laundering and terrorist financing. Controls put in place by these entities must be in proportion to identified risks. To comply with this requirement, entities must identify, assess, monitor, mitigate and manage the risk that their products and/or services may be abused by criminals for money laundering and terrorist financing. As a result, the accountable institution must assess all factors relevant to establishing a business relationship and/or conducting a single once off transaction with a client.

Client types: Accountable institutions must consider their different client types. For example, is the client a natural person or complex structure? From a money laundering and terrorist financing perspective, different client types present different levels of risk. Accountable institutions may find that dealing with a client who is a natural person presents less risk than dealing with a legal person such as a company. Some companies may be abused by criminal entities that attempt to hide behind the corporate structure. Accountable institutions must delve deeper to understand who their customers are, and the potential risks they pose. In light of this, it is vital that the accountable institution identifies beneficial owners of legal persons. Beneficial owners can include shareholders of companies and beneficiaries of trusts etc. In addition, they need to consider whether there is negative coverage on their clients in media, the client’s source of income and source of wealth. They need to ask, whether the client is in an occupation or sector that presents a higher risk from a money laundering and terrorist financing perspective. These questions help in identifying the risk when dealing with that client type.

Delivery channels: Accountable institutions must review the channels they use for on-boarding clients. Do they on-board clients through an intermediary or on a virtual platform with no face to face contact? The latter approach on-boarding clients may hold a higher risk than face to face on-boarding.

Geographic location: Accountable institutions must take into account their own location where they provide their products and services, in relation to where their client is located. Some accountable institutions do not necessarily provide products and services in different countries, in this instance the different provinces and even regions can be assessed and compared from a risk perspective. Some geographical locations may pose a higher risk due to a heightened perception of corruption, as well as lower levels of regulations regarding anti-money laundering and combating of terrorist financing.

Other factors, which should be considered include whether the client is a sanctioned person, a domestic prominent influential person, or a foreign prominent influential person. Accountable institutions may also refer to industry guidance (examples include the FATF guidance documents, and trends reports etc.) offered on whether a certain product, services, client types, or sectors and so on, pose a higher risk from a money laundering and terrorist financing perspective.

IDENTIFYING AND ASSESSING RISK

In order to identify risks, the accountable institution must assess all factors relevant to establishing a business relationship and/or conducting a single once off transaction with a client. Accountable institutions can take into account the following factors when identifying potential money laundering and terrorist financing risks:

- Products and/or services: Consider the extent to which the product/service offers anonymity to the client; does the product/service allow for third party payments; can the product be converted easily to cash; is the product/service subject to additional checks such as credit or regulatory approvals and so on. An overall assessment must be done on each of the accountable institution’s product and services, in order to help identify whether these products and services may be abused for money laundering and terrorist financing.

- Factors when identifying potential money laundering and terrorist financing risks: As a member of the FATF, South Africa is required to adhere to the Recommendations and standards set by the organisation.
After identifying and assessing the potential risks it faces, the accountable institution can then assign different weightings based upon the perceived risk, and an overall client rating. The higher the overall client rating, the more stringent the controls must be, enhanced control measures should be applied to mitigate the heightened risk. Where the client risk rating is lower, then the control measures may be lighter.

KEY ASPECTS TO MANAGING RISK

Accountable institutions must develop controls which mitigate and manage the risks, and which fulfil the FIC’s compliance requirements. Controls include but are not limited to policies, procedures, systems, training, reporting and other aspects. All controls implemented must be monitored to ensure that they are adequate and effective. All the controls developed and implemented by the accountable institution form part of their risk management and compliance programme (RMCP).

In summary, the controls that must be included in a RMCP must provide for:

- Client profiling – factors and methods to be taken into account when determining the overall client risk rating
- Customer due diligence, which includes identifying and verifying clients and all other required persons
- Additional due diligence, which includes identifying and taking reasonable steps to verify beneficial owners and other persons
- Enhanced due diligence, which includes obtaining senior management approval and putting in place any other enhanced measures to mitigate dealing with higher risk clients
- Simplified due diligence, which includes less stringent measures when dealing with lower risk clients
- Client transaction profiling methods, which includes profiling expected activity for products/services and client types
- Ongoing due diligence, which includes keeping client information up to date and accurate
- Account monitoring, where client products and services (i.e. accounts) are monitored to identify suspicious and unusual activity

- Client screening and payment screening against financial sanctions of the United Nations Security Council which is available on the UNSC and against the targeted financial sanctions list which is available on the FIC website at [www.fic.gov.za](http://www.fic.gov.za)
- Reports submitted to the FIC: Suspicious and unusual transactions reports, terrorist property reports, cash threshold reports and international fund transfer reports
- Keeping records of all customer information, transaction information and reports submitted to the FIC.

Accountable institutions must ensure its RMCP covers all the aspects as set out in section 42 of the FIC Act. The RMCP must be approved by the accountable institution’s board of directors, senior management or other person or group of persons exercising the highest level of authority in the accountable institution.