Business Risk Assessment Guideline

AML – CFT Department

1. Purpose and Scope

The purpose of this Guideline is to assist financial institutions in understanding and complying with their AML/CFT obligations relating to the requirement to conduct a Business-wide Risk Assessment under *Royal Decree No.30/2016* (“AML/CFT Law”) and Decision No E/80/2021 *Instructions to the Capital Markets Institutions* and *Decision No E/81/2021 Instructions to the* **Insurance and Takaful Companies, Brokers and Agents**. This Guideline sets out the expectations of the CMA regarding the factors that financial institutions should take into account when conducting their business wide risk assessment. The factors and measures described in this Guideline are not exhaustive and this Guideline does not set limitations on the steps to be taken by financial institutions in order to meet their statutory obligations. There is no standard risk assessment methodology and in conducting their risk assessment, financial institutions should consider any other factors and measures as appropriate to their business. Financial institutions should also have regard to the *AML/CFT Guidance for Financial Institutions* when conducting the business-wide risk assessment.

2. CMA Expectations

The business-wide risk assessment (BRA) must:

- Be documented
- Be specific to your business
- Include an assessment of the ML and TF risk posed by all of the below risk factors:
    - customers,
    - products and services,
    - transactions,
    - delivery channels,
    - geography,
    - new developments and technologies,
    - emerging ML/TF risks and
    - any other factors relevant to the business
- Assess and clearly differentiate between ML and TF risk

- Take into account the ML/TF National Risk Assessment of Oman as well as CMA Sectoral Risk assessments and other relevant sources of information
- Be reviewed and updated on a regular basis
- Approved by senior management

3. Overview of Business-Wide Risk Assessment

Financial Institutions must ensure that they have a **comprehensive understanding of the ML/TF risks** to which they are exposed, which is an important first step in applying the risk-based approach. Having a **well-documented ML/TF risk assessment** in place is central part of a financial institution meeting its AML/CFT obligations and should assist financial institutions in;

- understanding the ML and TF risks to which the entire business is exposed,
- determining how these risks are effectively mitigated through internal policies, procedures and controls and
- establishing the residual ML/TF risks and any gaps in controls that should be addressed.

Financial institutions must ensure that their BRA is **tailored to their business profile** and takes account of the factors and risks specific to their business.

Where a financial institution is part of a group, the financial institution should ensure that the group-wide risk assessment is sufficiently granular and specific to the individual financial institutions business and ML/TF risks to which it is exposed.

A generic ML/TF risk assessment that has not been adapted to the specific needs or business model of the financial institution will not meet the expectations of the CMA.

Financial institutions should note that ML/TF risk cannot be entirely eliminated regardless of how effective the AML/CFT control framework is.

4. Stages of an ML/TF business-wide risk assessment

A financial institution's risk assessment should consist of the following steps:

1. **Identifying, assessing and understanding the inherent ML and TF risks** (the risk of ML and TF occurring without consideration of any controls or mitigant in place to alter the likelihood or impact of the risk) across the business
   - Data used should include up to date quantitative and qualitative information - for example, types and numbers of customers, volume of operations for the types of customers, volume of business per product and service and geographic locations.
   - See Section 5 below

2. **Determining the nature and intensity of risk mitigating controls** to apply to the inherent risks
   - The level of inherent ML/TF risk influence the type and levels of AML/CFT resources, controls and risk mitigation strategies which are required to be put in place

3. **Risk monitoring and review**
   - The BRA is a cyclical process and the risk assessment should remain under regular review and whenever there are major developments in management and operations (e.g. business model, clientele, risk exposure, etc.). Financial institutions should also develop a list of trigger events that trigger ad hoc review

- The results of an effective ML/TF BRA will be the classification of identified risks into different categories, such as High, Medium and Low or some combination of those categories (such as medium-high, medium-low).

- An effective ML/TF BRA will allow the financial institution to make informed management decisions regarding risk appetite, allocation of AML/CFT resources and development of ML/TF risk mitigation strategies.

- Where higher risks are identified, the financial institutions must take enhanced measures to mitigate these risks.

- The risk that remains after all measures have been implemented effectively is known as the **residual risk**. The residual risk rating will always be more influenced by the level of inherent risk rather than the quality of controls.

5. Sources of Information

When financial institutions are conducting their risk assessment, they should have regard to **various relevant sources** of information. Examples include:

- Oman's National Risk Assessment of Money Laundering and Terrorist Financing (NRA)
- Any topical risk assessments (legal persons and legal arrangements, TF risk assessment, PF risk assessment)
- CMA sectoral risk assessments
- National Risk Assessment of other jurisdictions in which the financial institution operates or the customers are based
- Communications issued by the National Centre of Financial Information (NCFI)
- Guidance, circulars and any other communication from CMA or other relevant supervisory authorities
- Information from industry bodies or representatives
- Information from international standard setting bodies and international organisations, mutual evaluation reports of other jurisdictions and any typologies reports.
- The financial institution's own knowledge and expertise
- Any other credible and reliable sources

6. Inherent Risk Factors to consider when conducting an ML/TF BRA:[1]

a) Structural Risk
b) Customer risk
c) Products, service and transaction risk
d) Delivery channel risk
e) Geographic risk
f) New and existing technologies risk

a) Structural Risk

[1] Financial institutions should note that all of these Risk Factors are examples of what should be considered at a minimum.

Examples of data which should be collected and assessed	Quantitative information
• Nature of the business • Size/scale of the business • Diversity and complexity of business lines • Diversity and complexity of markets in which the company operates	• Annual turnover • Annual net profits • Number of employees • Number of branches or offices • Number of markets in which the company operates • Number of different business lines • Total Assets, overall and per business line/market

b) Customer risk factors

Examples of data which should be collected and assessed	Quantitative information
• Total number of customers • Type of customer (natural persons, legal persons, legal arrangements) • Non-resident customers • PEPs (foreign, domestic, international organisations; customers and BOs of customers) • High net worth individuals • Cash intensive business • Special Purpose Vehicles • NPOs • Other high-risk businesses and links to sectors which are commonly associated with higher level of ML/TF risk (e.g. dealers in precious metals or stones; money remitters)	• Number of customers (individuals, legal persons and legal arrangements in the categories mentioned • Total number of transactions • Total value of transactions • Total number of assets

• Legal person customers with nominee shareholders or nominee directors • Persons acting as representatives/nominees on behalf of the customer • Customers with complex ownership structures • Holders of bearer shares or other bearer negotiable instruments	

c) Product/services/transaction risk factors

Examples of data which should be collected and assessed	**Quantitative information**
• Complexity of the product, service or transaction • Level of transparency of the product, service or transaction and extent that the product, service or transaction might facilitate or allow anonymity or opaqueness of the customer, ownership or beneficiary structures • Wire transfers • Private banking/wealth management • Credit cards • Prepaid cards • Correspondent banking services/transactions • Trade finance transactions • Means of payments: Bank Transfers, Cheques, Prepaid cards, Virtual currency, etc.	• Number of products issued • Number of customers (natural person, legal person, legal arrangement) per product/service • Transaction value per product/service • Number of transactions per each payment means • Volume of funds transferred per each payment means; • Profile of customers that use particular payment means

d) Delivery Channel risk factors

Examples of data which should be collected and assessed	Quantitative information
• Direct onboarding of customer • Non-face to face onboarding of customer • Internet banking • Mobile banking • Use of introducers, intermediaries and/or agents • Reliance on third parties for CDD • New and untested delivery channels	• Number of business relationships that have been entered into face to face • Number of business relationships that have been entered into non- face to face • Number of customers (natural persons, legal persons and legal arrangements) onboarded through each delivery channel • Number of introducers, intermediaries and/or agents • Introducers, intermediaries and/or agents geographies • Third parties’ geographies • Profile of the customers that came through each delivery channel

e) Geographic risk factors

Examples of data which should be collected and assessed	Quantitative information
• Countries subject to sanctions – TF and PF • FATF blacklisted/grey-listed countries • Offshore jurisdictions • Tax non-compliant jurisdictions • Countries associated with high level of corruption or organized crime	Country breakdowns for - Customers (natural persons, legal persons and legal arrangements) - Beneficial owners of customers - Transactions (incoming and outgoing) - Products and services - Trade finance - Correspondent relationships

• Countries associated with high TF risks • High Risk countries as identified by the Committee under Article 13(k) of the AML/CFT Law	- Introducers, agents, etc.

f) New products and new technologies risk

The AML/CFT Law and Instructions require financial institutions to identify and assess the ML and TF risks that may arise from the development of a new product, service, business practice or delivery mechanism and from the use of a new or developing technology for new or pre-existing products or services. Financial institutions must complete the assessment of such risks and take the appropriate risk management measures, **prior** to launching new products and services, practices, techniques or technologies. Such risk assessments must be documented and updated as necessary.

7. Emerging ML and TF Risk

Financial institutions should ensure that they have systems and controls in place to identify and assess emerging ML and TF risks or existing ML and TF risks which have increased and where appropriate incorporate them into the BRA in a timely manner. Such systems and controls may include:

- Processes to ensure that internal information is reviewed regularly to identify trends and emerging issues
- Processes to ensure that the financial institution regularly reviews information from various sources (examples provided in Section 5).
- Processes to capture and review information relating to new products and technologies
- Engagement with industry representatives, supervisory authorities, law enforcement agencies and processes to feed back any findings to relevant employees
- The establishment of a culture of information sharing and strong ethics within a financial institution

8. Weighting of the Risk Factors

When assessing ML/TF risk, financial institutions may decide to weight risk factors differently depending on their relative importance.

When weighting risk factors, financial institutions should consider the relevance of different risk factors in the context of a business relationship or transaction. The weight given to each of these factors is likely to vary from product to product and customer to customer (or category of customer) and from one financial institution to another. **When weighting risk, financial institutions should ensure the following:**

- Weighting is not unduly influenced by just one factor;
- Economic or profit considerations do not influence the risk rating;
- Weighting does not lead to a situation where it is impossible for any business relationship to be classified as high risk;
- Situations identified by the AML/CFT legislation and/or Instructions as always presenting a high ML or TF risk, cannot be over ruled by the firms weighting;
- Financial institutions can override any automatically generated risk score where necessary. The rationale for the decision to override such scores should be governed and documented appropriately.

Where financial institutions use **automated IT systems** to allocate overall risk scores to categorise business relationships or transactions and do not develop these inhouse but rather purchase them from an external provider, they should ensure that:

- The financial institution fully understands the risk rating methodology proposed by the external provider and how it combines risk factors to achieve an overall risk score;
- The methodology which is used meets the financial institution’s risk assessment requirements and legislative obligations;

- The financial institution can satisfy itself that the scores allocated are accurate and reflect the financial institutions understanding of ML/TF risk.

9. Risk Mitigation

Financial institutions should ensure that they have appropriate policies, procedures and controls in place to effectively manage and mitigate the ML/TF risks which they have identified, including the risks which have been identified at a national level. The policies, procedures and controls should be approved by senior management. They should be **appropriate and proportionate** to the risks identified and should be subject to ongoing monitoring and review to ensure that they continue to effectively manage and mitigate the level of risk identified.

Below is an example of an Internal Control Assessment:

AML/CFT Obligation	[2]Examples of factors which should be considered
AML-CFT governance	Updated Policies & Procedures in place, Assessment of new products and services, delivery channels, risk assessment update, board oversight, MLRO reports, board members and senior management understand AML/CFT obligations and responsibilities
KYC/CDD/EDD process	Onboarding of customers meet AML/CFT obligations (for example complete data, correct feeding, timely review conducted, assessment of identification of beneficial owners complete
TFS	TFS Screening, Pending sanction alerts, effectiveness of the current threshold, last update, any regulatory findings, procedures in place for positive hit, understanding of difference between TF and PF sanctions,
PEPs	Risk management system to identify whether customer or BO is a PEP, screening, senior management approval, source of wealth and source of funds always established, EDD.
Transaction Monitoring	Scenario tuning, performance, quality amount of pending alerts, time spent for alert closure, pending cases, new scenarios, review by the quality assurance, audit and regulatory findings, measure the number of alerts generated

[2] Financial institutions should note that these are minimum factors which should be considered as part of the Internal Control Assessment.

	unreasonable to the institution’s size. Number of customers risk rating/profile changed as a result of the transaction monitoring.
MLRO Role	Independent and adequate authority, Appropriate qualifications and experience, functions documented.
Training	Documented training programme in place, Nature and type of training, training differentiates between CTF and AML, training includes TF sanctions and PF sanctions, assessment and pass score, training topics, tailored to different categories of employee, frequency and delivery method of the training, number of staff attending training, training for the board.
STR Reporting	Quality assurance and NCFI feedback, quality, timing and volume of STR reported, size of STRs reported vs total alerts generated and institution’s size, initial date of the transaction vs STR reporting date. List of indicators and grounds for suspicion. Number of STR returned by NCFI/Request for information and assessment of the reasons why had been retained. Timing of response to NCFI requests. Number of exited relationship or changes in risk rating based of STR filled, records of analysis.
Audit and Independent testing	Independent audit function, frequency of testing, independent test of scenarios and alert quality, screening system, CDD accuracy, thresholds, risk rating, STR reporting, testing of new scenarios, ensure all customers and transactions are mapped to the transaction monitoring system

10.Approval and communication of the BRA

The BRA should be documented and made available to the CMA as requested.

Senior management within the financial institution must be made aware of the results of the BRA and be provided with enough information to understand and approve the risk assessment.

It is also important that **employees** are made aware of the results of BRA, for instance through the ongoing employee ML/TF training programme. This ensures that employees are aware of the main risks that their institution is exposed to and that they can effectively execute the policies, procedures and controls determined by senior management to mitigate the risks.

11.Review and updating of the BRA

As ML/TF risks are always changing, the ML/TF risk assessment should be subject to **regular review and approval** to ensure it adequately reflects the ML and TF risks to which the financial institution is exposed. Where a financial institution is aware that a new risk has emerged, or an existing one has increased, this should be reflected in the risk assessment as soon as possible. Financial institutions should also assess information obtained as part of their ongoing monitoring of a business relationship and consider whether this affects the risk assessment.

Financial Institutions should ensure that they have systems and controls in place to ensure that their risk assessment remains up to date. For example, setting a timeline as to when the next BRA will take place to ensure changing, new or emerging risks are include. Any update to the BRA, just like the original risk assessment, must be documented, and commensurate to the ML/TF risk.