CBUAE Classification: Public

CBUAE OUTREACH EVENT
on
Financial Crimes Institutional Risk Assessments for LFIs

18 August 2021

CBUAE Classification: Public

Outline of this Presentation

- Introduction
- The Risk-Based Approach and the Institutional Risk Assessment Process
- Assessing Inherent Risks
- Assessing Mitigating Measures
- Assessing Residual Risk and Using Risk Assessment Results
- Q & A

Purpose & Applicability of the Outreach Event

Purpose

- The guidance offered in this presentation does NOT constitute regulation and does NOT introduce new legal obligations.
- It is designed to help CBUAE's LFIs understand the purpose and context of their existing legal obligations, as well as the CBUAE's expectations for how those obligations will be fulfilled.

Applicability

The guidance applies **to all financial institutions licensed or registered by the CBUAE.**

This presentation is based on the CBUAE's *AML/CFT Guidelines for Financial Institutions*. LFIs should consult this document for additional detail and guidance regarding the institutional risk assessment process.

CBUAE Classification: Public

The Risk-Based Approach and the Institutional Risk Assessment Process

CBUAE Classification: Public

What is the Risk-Based Approach?

- LFIs are expected to **identify, assess, and understand** the money laundering, terrorist financing, proliferation financing, sanctions, and bribery and corruption risks (collectively, "illicit finance risks") to which they are exposed and **apply mitigating measures** that are commensurate with those risks.
- The risk-based approach (RBA) allows LFIs to adopt a **more flexible** set of measures in order to target their resources and apply mitigating measures more effectively: it is not a "one size fits all" approach.

The Role of the Risk Assessment

- **The risk assessment forms the basis of an LFI's RBA**, in that it enables the LFI to understand its particular illicit finance risks and implement mitigating measures to address those risks.
- Specifically, the risk assessment should allow an LFI to **allocate human and technical resources** in a manner commensurate with its illicit finance risks.
  - Where LFIs identify **higher risks**, the range, degree, frequency, or intensity of the LFI's controls should be stronger.
  - Where LFIs identify **lower risks**, they may decide to implement simplified measures, consistent with minimum legal obligations.

Risk Assessment Obligations in the UAE

AML-CFT Law, Article 16.1

Each LFI is obliged to "[i]dentify the crime risks within its scope of work as well as **continuously assess, document, and update such assessment** based on the various risk factors established in [implementing regulations] and maintain a risk identification and assessment analysis with its supporting data to be provided to the Supervisory Authority upon request."

AML-CFT Decision, Article 4.1

LFIs "are required to identify, assess, and understand their crime risks in concert with their business nature and size, and comply with the following:

(a) Considering all the relevant risk factors such as **customers**, **countries or geographic areas**; and **products**, **services**, **transactions** and **delivery channels**, before determining the level of overall risk and the appropriate level of mitigation to be applied.

(b) Documenting risk assessment operations, keeping them up to date on on-going bases and making them available upon request."

Overview of the Risk Assessment Process

Inherent Risk Assessment

- Inherent risks are the illicit finance risks presented by an LFI's customers, products, services, transactions, delivery channels, geographies, *and all other relevant factors* **before accounting for control measures in place** to mitigate these risks.
- An assessment of inherent risks should take into account the **threats** facing the institution, sector, and jurisdiction and the LFI's particular **vulnerabilities** to abuse by illicit actors.

Mitigating Measures Assessment

- Mitigating measures are the **counter-illicit finance policies, procedures, and controls** in place to mitigate the illicit finance risks facing the LFI.
- Mitigating measures include appropriate **governance and management oversight**, **customer due diligence**, **internal controls**, **training**, and **independent audit**.

Residual Risk Assessment & Follow-Up

- Residual risks are the risks remaining **after accounting for the effectiveness of controls** and other mitigating measures.
- LFIs are expected to ensure that their residual risks remain within their **risk appetite**, to allocate additional **resources** to areas of higher risk, and to **remediate** any identified deficiencies.

Risk Assessment Methodology

- LFIs may utilize a variety of models or methodologies to assess their risks, in keeping with **the nature and size of their business**.
  - In all cases, an LFI should **document** the risk assessment methodology and its underlying rationale.

- An effective methodology should:
  - Reflect input from **internal sources**, such as the AML/CFT compliance officer and relevant risk units, as well as information from **external sources**, such as the National Risk Assessment (NRA), topical risk assessments, official guidance or notices, and bodies such as the FATF;
  - Describe the selection and weighting of **risk factors** and reflect the LFI's **risk appetite**;
  - Be based on **quantitative and qualitative data and information**, make use of internal interviews, questionnaires, and audit reports, and provide for quality assurance review;
  - Provide for **separate, tailored assessments of different business lines or segments** that have different risk profiles before consolidating into a unified view.

- Additionally, LFIs with oversees branches, subsidiaries, or other affiliates or legal entities should perform **separate assessments for each entity** before consolidated them into a unified, group-wide view.

- A more detailed description of an effective risk assessment methodology is provided in the CBUAE *AML/CFT Guidelines for FIs*, section 4.2.1.

Risk Assessment Frequency, Updating, and Follow-Up

Frequency

- LFIs should decide on the frequency of their financial crimes risk assessment, taking into account their size, the nature of their business, their inherent and residual illicit finance risks, and the results of the NRA and topical risk assessments.
- **In most cases, LFIs should consider performing their risk assessments at least annually**, although more or less frequent assessments may be justified by particular circumstances.

Documentation and Updating

- LFIs are obliged to **document their risk assessments**, including the methodology, analysis, conclusions, and supporting data.
- LFIs are also obliged to **keep their risk assessments up to date**, including by:
  - Periodically reviewing risk assessment methodologies; and
  - Updating the risk assessment following material changes to the business or risk or regulatory environment.

Follow-Up

- LFIs must also perform and document relevant follow-up actions, including:
  - **Reporting RA findings** to the board (or board committee) and senior management;
  - Ensuring residual risks remain within the LFI's **risk appetite**;
  - **Allocating additional resources** to areas of higher risk; and
  - **Undertaking and tracking corrective actions** to address control deficiencies.

CBUAE Classification: Public

Assessing Inherent Risks

Customers

- **LFIs should understand the risks of their customer base, including by identifying certain categories of customers as inherently higher risk**, considering the results of the NRA, official guidance and notices, and global standards documents such as FATF guidance.
- Specific customer risk factors may include:
  - Customers with complex legal or ownership structures;
  - Customers associated with higher-risk persons or professions, such as politically exposed persons (PEPs);
  - Nonresident entities, particularly those with connections to higher-risk jurisdictions;
  - Professionals (such as lawyers, accountants, and other DNFBPs) acting as intermediaries on behalf of their underlying customers;
  - High-net-worth individuals; and
  - Foreign financial institutions, especially those in higher-risk jurisdictions.
- In addition to considering the **type** of customers with which it does business, an LFI may consider the **size** of its customer base and the **maturity** of its customer relationships (e.g., longer-term vs. one-off customers).

Segmenting and Risk-Rating Customer Types

- At a minimum, each LFI should **identify types or categories of customers that present heightened illicit finance risks** for the purposes of "segmenting" and risk-rating customers at onboarding.
  - Larger or more complex LFIs should consider applying risk scores to all customer types, rather than simply distinguishing higher-risk from non-higher-risk customer types.
  - For example, a **bank** may assign the following risk scores to various customers it serves, based on its assessment of their inherent illicit finance risks:

Customer Type	Customer Risk Score (0-1)
Dealers in precious metals and stones	1.0
Customers in a jurisdiction rated as "high risk"	1.0
Money services businesses	0.9
Politically exposed persons (foreign)	0.8
Politically exposed persons (domestic)	0.6
State-owned enterprises (foreign)	0.6
State-owned enterprises (domestic)	0.5
Publicly-traded companies	0.2

CBUAE Classification: Public

Banking Example (cont'd)

Customer Type	Customer Risk Score	% of Customer Base	% of Transactions by Value	Exposure Score	Inherent Risk Score
Dealers in precious metals and stones	1.0	10	5	7.5	7.5
Customers in a jurisdiction rated as "high risk"	1.0	15	2	8.5	8.5
Money services businesses	0.9	5	20	12.5	11.25
Politically exposed persons (foreign)	0.8	1	5	3	2.4
Politically exposed persons (domestic)	0.6	9	12	10.5	6.3
State-owned enterprises (foreign)	0.6	6	1	3.5	2.1
State-owned enterprises (domestic)	0.5	15	20	17.5	8.75
Publicly-traded companies	0.2	45	40	42.5	8.5
				Overall (0-100+)	**55.3**

Geographies

- LFIs should consider geographic illicit finance risk factors from both **domestic** and **cross-border** sources.
- Geographic risks arise from the locations **where the LFI has offices, branches, and subsidiaries**, as well as the locations **where their customers reside or conduct their activities**.
- In assessing the risk of a particular geography, LFIs may consider:
  - The strength of the country's AML/CFT regulatory framework;
  - Whether the country is subject to international sanctions;
  - The country's reputation and track record regarding ML/TF/PF, corruption, and corporate transparency; and
  - The interaction between geographic and customer risks (e.g., a complex legal entity located in a country with poor corporate transparency).

Products, Services, and Transactions

- LFIs should review their **lines of business**, **products**, and **services** to identify those most vulnerable to abuse by illicit actors or for illicit purposes.
- Specific product, service, and transaction risk factors may include:
  - Whether the product, service, or transaction type is **associated with any established illicit finance typology** (e.g., as provided in the CBUAE *AML/CFT Guidelines for FIs*, section 3.10);
  - The **complexity** of the product, service, or transaction type, including dependencies on multiple systems and/or market participants;
  - The **transparency and transferability of ownership or control** of the product, service, or transaction type, including opportunities for funds to be pooled, co-mingled, or transferred anonymously; and
  - The **size or value parameters or limits** of the product, service, or transaction type.

Delivery Channels

- LFIs should evaluate the risks associated with different channels for the **acquisition and management of customers** and the **delivery of products and services**.
- LFIs should pay particular attention to channels that favor **anonymity** or place **third-party intermediaries** between the LFI and the customer, including:
  - Non-face-to-face channels (especially those without safeguards such as electronic identification systems);
  - The use of third-party business introducers, intermediaries, agents, or distributors; and
  - The use of third-party payment processors, systems, or other intermediaries.

Delivery Channel Risk: Insurance Example

- Like other LFIs, insurance companies should identify and document all delivery or distribution channels that may present heightened illicit finance risk and assess their overall exposure to such channels.

Delivery Channel Risk Attribute	Delivery Channel Risk Score (0-1)	% of GWP Sold via Channel	Inherent Risk Score
Use of distributor that is not subject to AML/CFT obligations or has no AML/CFT program	1.0	10	10
Customer pays the distributor, who then pays the insurer (rather than paying the insurer directly)	0.8	45	36
Insurance sold via non-face-to-face channels (e.g., online or by phone)	0.6	65	39
Use of channels with no higher-risk attributes	0.1	20	2
		Overall (0-100+)	**87**

New Products, New Technologies, and Other Emerging Risks

- LFIs should assess such risks **prior to launching new products, services, or other technologies** (e.g., via a “new product committee” or other approval process).
- LFIs should consider their **depth of experience and expertise** with a new product, service, transaction type, or delivery channel, as well as the vulnerability of such new features to abuse by cyber criminals.
- LFIs must **review and update the risk assessment**—and adjust their mitigating measures, as needed—following the introduction of new products or services, new technologies or delivery processes, or the establishment of new branches and subsidiaries.

CBUAE Classification: Public

Assessing Mitigating Measures

Essential Elements of an AML/CFT Compliance Program

Governance	• Appointment of a compliance officer (with prior consent of Supervisory Authority); group oversight; reporting to senior management and the Board of Directors
Customer Due Diligence	• Customer and beneficial owner identification and verification; establishing a customer risk profile; ongoing monitoring and updating; risk-based EDD and SDD
Internal Controls	• Suspicious transaction/activity monitoring and reporting; sanctions name/transaction screening; testing of TM and sanctions screening systems; recordkeeping
Training	• New hire and role-specific training on the LFI's policies, procedures, and risks; training for the Board and senior management
Independent Audit	• Periodic, risk-based independent testing or auditing of the AML/CFT function

Mapping of Mitigating Measures to Inherent Risks

- Because different controls are needed to manage different types of illicit finance risk, LFIs should **map specific controls or control areas to specific inherent risks** and ensure that controls are **appropriately tailored** to each of the LFI's inherent risks at a granular level.
  - For example, strong beneficial ownership identification and verification procedures are an effective control for the risks presented by shell or front companies but do not help mitigate the risks associated with high-risk natural person customers such as PEPs.
  - Similarly, transaction monitoring rules cannot be "one size fits all," but must be tailored to the specific risks, patterns, and typologies relevant to the specific LFI.
- A careful mapping of controls to inherent risks will help ensure adequate controls **coverage** and assist in the assessment of **residual risk** and the risk-based allocation of resources during the **follow-up** stage.

Example: Mapping Controls to Customer Risk

- Although controls related specifically to CDD will clearly be relevant to the mitigation of an LFI's inherent customer risks, the LFI should consider how other elements of its AML/CFT program contribute to the full and effective management of such risks across the entire customer lifecycle.

Inherent Risk Category	Corresponding Control Factors	Weight of Each Factor	Control Rating (0-100)
Customers	Customer ID&V	15%	90
	BO ID&V	15%	50
	Customer Risk Profile	15%	44
	CDD Updating	10%	60
	Name Screening	10%	70
	EDD	10%	14
	CDD Training	10%	5
	CDD-based TM	5%	18
	Staffing & Resources	10%	55
		Overall	**48.9**

Score	Rating
0-25	Ineffective
25-50	Partially Effective
50-75	Largely Effective
75-100	Effective

CBUAE Classification: Public

Assessing Residual Risk and Using Risk Assessment Results

Calculating Residual Risk

- **Residual risk** is the illicit finance risk remaining **after** accounting for the effectiveness of mitigating measures.
  - Residual risk may be calculated at the level of **individual risk factors** (i.e., customers, products and services, etc.) and for **the LFI as a whole**.
  - Larger or more complex institutions should assess residual risk at the level of **particular business lines** before consolidating into a unified view.

Example: Residual Customer Risk

- To return to our banking example, **inherent customer risk** received a score of 55.3, corresponding to a risk rating of **High** for this risk factor (where 0-25 = Low; 25-50 = Medium; 50-75 = High; and 75-100+ = Very High).
- **Controls related to customer risk** received a score of 48.9, corresponding to a risk rating of **Partially Effective** for this risk factor (where 0-25 = Ineffective; 25-50 = Partially Effective; 50-75 = Largely Effective; and 75-100 = Effective).
- Based on these ratings and the residual risk matrix provided below, **residual customer risk** is therefore assessed to be **High.**

		Control Effectiveness			
		Ineffective	Partially Effective	Largely Effective	Effective
Inherent Risk	Very High	Very High	Very High	High	Medium
	High	High	High	Medium	Medium
	Medium	Medium	Medium	Low	Low
	Low	Low	Low	Low	Low

Sample residual risk 'matrix'

- **Note that the LFI's analysis of *why* it arrived at a given assessment of residual risk is just important as the headline assessment itself**, as this analysis will allow the institution to appropriately enhance controls and better mitigate its particular risks.
- Risk ratings for individual risk factors can then be aggregated to calculate **business line risk** (where applicable) and overall **institutional risk**.

Using Risk Assessment Results

Developing and Implementing Corrective Action Plans

- LFIs should develop and document **corrective action plans** for any material risk assessment finding.
- Larger or more complex institutions may consider assigning priority scores or ratings to individual findings to ensure that remediation activities target the most serious risks.
- Corrective action plans should be **closely tracked** and completed actions should be **supported with evidence and documentation**.

Reporting to Senior Management and the Board

- Risk assessment findings and remediation activities should be **reported to the board (or board committee), where applicable, and to senior management** to ensure adequate oversight and allocation of resources.

Reallocating Resources and Ensuring Consistency with Risk Appetite

- LFIs should ensure that the **allocation of human and technical resources** are based on and commensurate with the findings of the risk assessment, and that any residual risks remain within the LFI's **risk appetite**.

CBUAE Classification: Public

Questions