

Financial Crime Prevention Outreach Session #3



ABU DHABI GLOBAL MARKET
سوق أبوظبي العالمي

Financial Crime Prevention Unit

14 October 2019

FINANCIAL SERVICES REGULATORY AUTHORITY
سلطة تنظيم الخدمات المالية

Agenda



- National Risk Assessment
- Sanction monitoring and obligations under UAE Cabinet Res. No (20) of 2019
- goAML system
- Thematic Review

Provide an update on the NRA

01

National Risk Assessment



What is the NRA?



Objective of NRA



The main objective for NRA are:-

Identifying vulnerabilities, threats and risks

- To mitigate and take administrative and other measures

Is a tool for policy Makers

- To determine how financial and human resources are distributed

Provide clear idea of the risk scale

- To facilitate the effectiveness of the risk based process

The importance National Risk Assessment



Have a more comprehensive and common understanding of the inherent risks

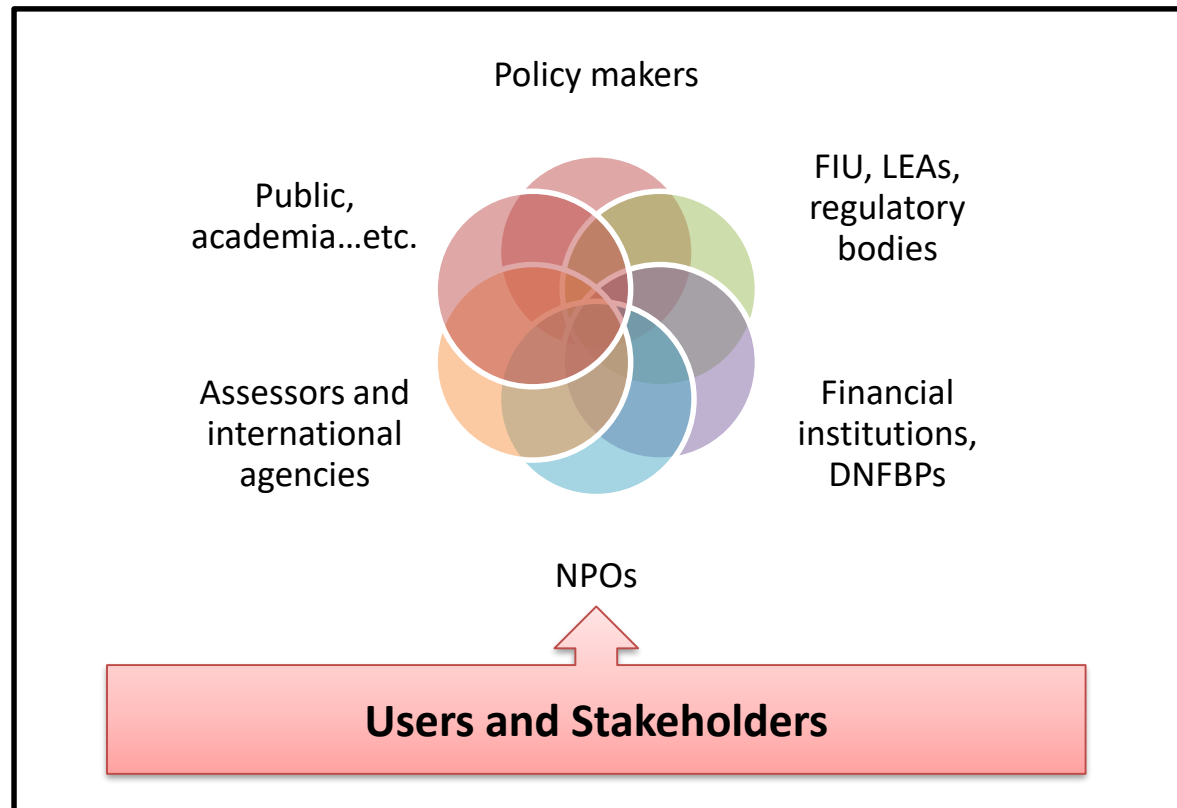
Provides the basis for the formulation policies and procedures

Allows country to make more informed judgement about level of remaining risks or residual risks



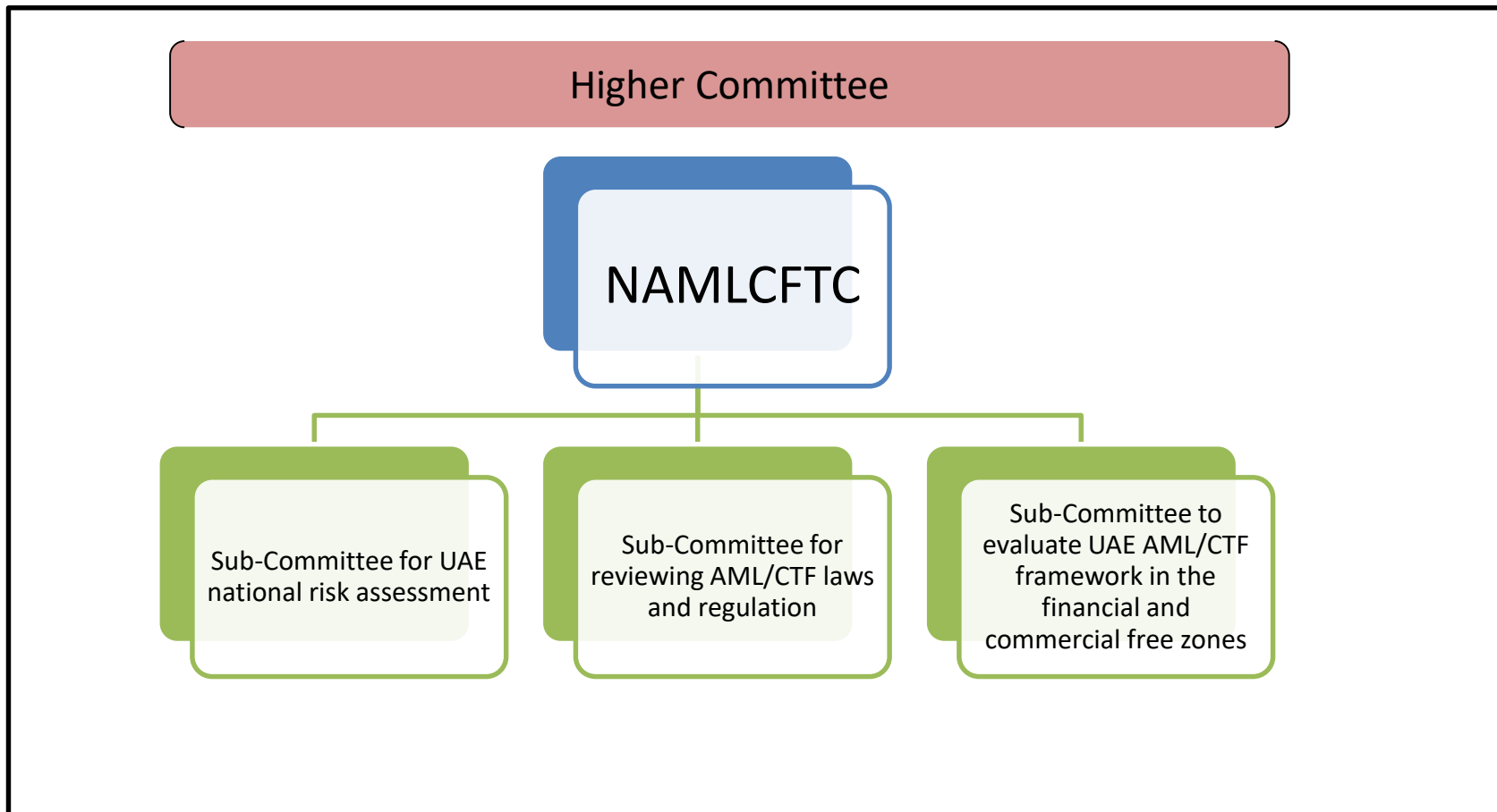
National ML and TF Risk Assessment

- The first UAE's NRA-related work started
- The Key Users and Stakeholders have been involved





- **Governance**



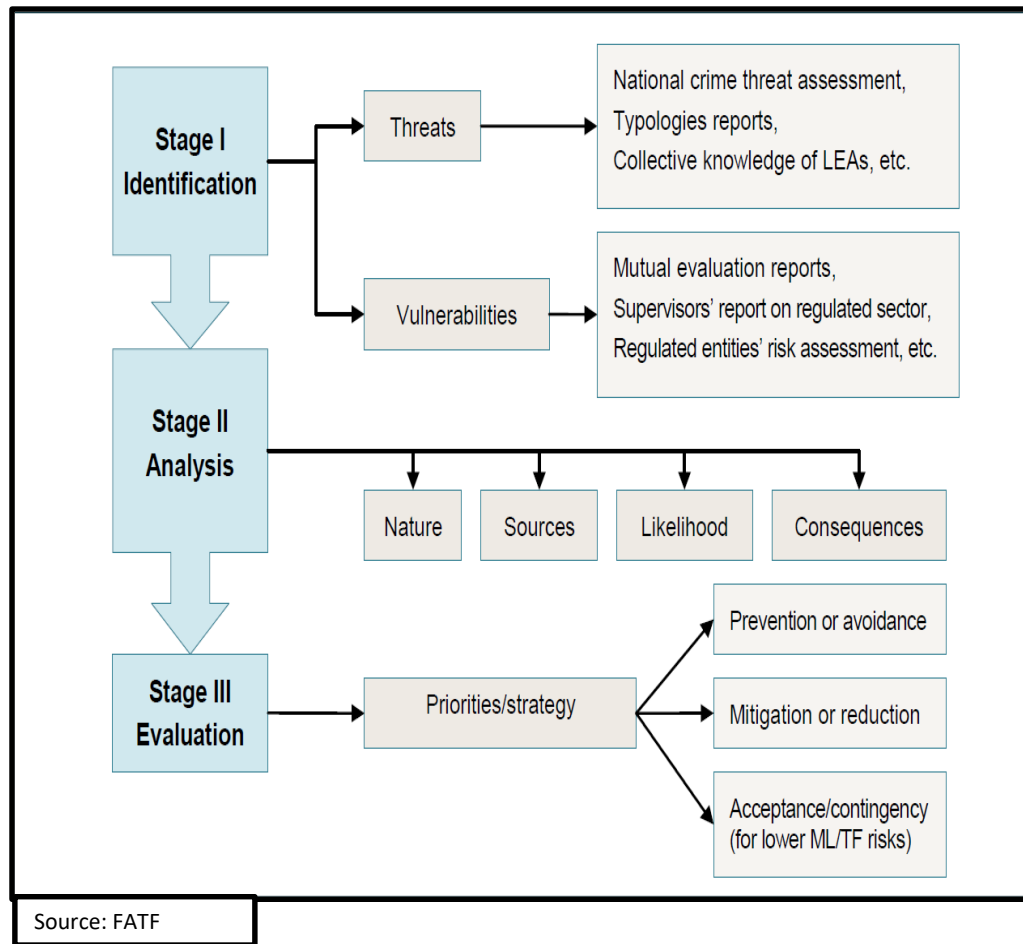
National ML and TF Risk Assessment-Stages



- National Inherent Risk Assessment is key to support Risk-Based Approach

- Developing profiles for each main elements of risk to be assessed:

- ML Threats
- TF Threats
- Sectoral Vulnerabilities
- National Vulnerabilities
- Consequences
- Rate each factor in the profile
- Rate confidence in information



The NRA Methodology - ML Threats



- The UAE authorities identified the threats for the 21 predicate crimes

High	medium-high	medium	low
<ul style="list-style-type: none"> Fraud Counterfeiting and Piracy of Products Illicit Trafficking in Narcotic Drugs and Psychotropic Substances Professional Third Party Money Laundering. 	<ul style="list-style-type: none"> Market Manipulation Robbery or Theft Illicit Trafficking in Stolen and Other Goods Forgery Smuggling (including in relation to customs and excise duties and taxes) Tax crimes (related to direct taxes and indirect taxes) Terrorism including Terrorist financing 	<ul style="list-style-type: none"> Extortion Trafficking in Human Beings and Migrant Smuggling Corruption and Bribery Sexual Exploitation including Sexual Exploitation of Children Illicit Arms Trafficking Counterfeiting Currency 	<ul style="list-style-type: none"> Murder Grievous Bodily Injury Kidnapping Illegal Restraint Hostage-taking, Piracy Environmental Crime

- The UAE authorities used the pre-defined rating criteria to be assessed ML Threats:
 - Actor's Capacity
 - Scope of ML activity
 - Proceeds of Crime

The NRA Methodology - TF Threats



The NRA also considered the risks associated with Terrorism Financing.

The Rating Factors for TF are:

Factor	Definition
Terrorist Actors' Capacity	sophistication, network and resources contribute to resilient, organization structure, size and complexity.
Scope – global reach	A network support (local, regional, national, transnational) contributing to the resilience.
Estimated of fund raised in the country annually	Estimated Dhs value of funds raised in the country

The NRA Methodology - Sectorial Vulnerabilities



The UAE authorities also identified inherent ML/TF sectorial vulnerabilities based on 5 pre-defined rating criteria:

Factor	Definition
Inherent characteristics	Economic significance, complexity of business structure, integration with other sectors.
Nature of products and services	Products and services offered are more vulnerable to ML/TF, such as: cash payments, private banking, trade finance services, cross-border movements, high value commodities, professional services, corporate structures.
Nature of clientele	Sector's clientele profile, business relationship, Customer employment status, client's occupation/businesses; facility to identify domestic / foreign PEPs, BOs.
Geographic reach	High risk jurisdictions, countries of concern for ML/TF, and countries of strategic concern.
Nature of delivery	Anonymity (non Face to face), face-to-face, use of third parties, Complexity (multiple intermediaries)

The NRA Methodology -National Vulnerabilities/identifying consequences



ML/TF risk factors related to national vulnerabilities:-

- Political
- Economic
- Social
- Technological
- Legislative



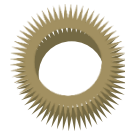
UAE ML Threats: Ratings



The UAE authorities identified the inherent vulnerability ratings for each sectors in relation to Money Laundering

High	medium-high	medium	low
<ul style="list-style-type: none"> • Fraud • Counterfeiting and Piracy of Products • Illicit • Trafficking in Narcotic Drugs and Psychotropic Substances • Professional Third Party Money Laundering. 	<ul style="list-style-type: none"> • Market Manipulation • Robbery or Theft • Illicit Trafficking in Stolen and Other Goods • Forgery • Smuggling (including in relation to customs and excise duties and taxes) • Tax crimes (related to direct taxes and indirect taxes) • Terrorism including Terrorist financing 	<ul style="list-style-type: none"> • Extortion • Trafficking in Human Beings and Migrant Smuggling • Corruption and Bribery • Sexual Exploitation including Sexual Exploitation of Children • Illicit Arms Trafficking • Counterfeiting Currency 	<ul style="list-style-type: none"> • Murder • Grievous Bodily Injury • Kidnapping Illegal Restraint • Hostage-taking, Piracy • Environmental Crime
UAE Vulnerabilities: Ratings (On-Shore)			
<ul style="list-style-type: none"> • Banks • Money Service • Business/Exchange Houses • Dealers in Precious Metals and Stones. 	<ul style="list-style-type: none"> • Financial Advisors/Consultancy, Investment Fund/Asset Management, Brokers and Agents, and Credit Providers (Finance Companies). • Lawyers, Notaries and Other Independent Legal Professionals • Real Estate Agents • Company Service Providers 	<ul style="list-style-type: none"> • Auditors • Custodians • Life Insurance/ Investment and Property and Casualty (General Insurance) 	
UAE Vulnerabilities: Ratings (FFZs)			
<ul style="list-style-type: none"> • Money Service • Businesses/Exchange Houses 	<ul style="list-style-type: none"> • Banking • Brokers and Agents • Wealth Management • Custodians • Investment Fund Management • Financial Advisors • Company Service Providers • Dealers in Precious Metals Stones • Real Estate Agents • Lawyers, Notaries and Other Independent Legal Businesses. 	<ul style="list-style-type: none"> • Auditors • Accountants • Insolvency Firms • Life Insurance 	<ul style="list-style-type: none"> • General Insurance

National ML and TF Risk Assessment



Outcomes of NRA – How it was useful?

- Prepared the country for the mutual evaluation
- Engaged all relevant authorities and shape the country's AML/CTF policy





Expectations of ADGM entities

1. Understand your inherent ML/TF risks
2. Apply the most effective measure to address your business risks.
3. Review and update your manuals to be align with NRA report.

Sanction monitoring and obligations under UAE Cabinet Res. No (20) of 2019

02



1. The U.A.E, as a member of the United Nations, is required to comply with all Sanctions issued and passed by the UNSC. The U.A.E periodically publicises its imposition of sanctions. These UNSC obligations apply in the ADGM and their importance is emphasised by specific obligations contained in the AML Rulebook requiring Relevant Persons to establish and maintain effective systems and controls to make appropriate use of UNSC Sanctions and resolutions (see Chapter 11).
2. The FATF has issued guidance on a number of specific UNSC Sanctions and resolutions regarding the countering of the proliferation of weapons of mass destruction. Such guidance has been issued to assist in implementing the targeted financial Sanctions and activity based financial prohibitions. This guidance can be found on the FATF website (at www.fatf-gafi.org).
3. In relation to unilateral Sanctions imposed in specific jurisdictions such as the European Union, the U.K. ("HM Treasury") and the U.S. (by the Office of Foreign Assets Control ("OFAC")) and any other Sanctions that may apply to the Relevant Person's business partners and customers, the Regulator expects a Relevant Person to consider and take positive steps to ensure compliance where required or appropriate.

The UAE Cabinet of Ministers have recently issued the following resolutions:



Resolution Number	Designated Persons
Resolution No. 18 of 2017	59 individuals and 12 entities
Resolution No. 28 of 2017	9 individuals and 9 entities
Resolution No. 45 of 2017	11 individuals and 2 entities
Resolution No. 53 of 2017	11 individuals and 2 entities
Resolution No. 24 of 2018	6 individuals and 3 entities
Resolution No. 50 of 2018	9 individuals



**Cabinet Resolution No. (20) of 2019
Concerning Regulations of Terrorism Lists, Enforcement of the
Security Council Resolutions Concerning Terrorism Combatting,
Prevention and Financing, Stop of Spread and Financing of Weapons
and the Relevant Resolutions**

- Obligations of Financial Institutions and Designated Non-Financial Businesses and Professions

Continuation of Slide 2



Article (19)

For the purposes of enforcement of the provisions of this Resolution, financial institutions and designated non-financial businesses and professions shall:

1. **Update the details** of the persons listed on the Sanctions Committees on a daily basis, by referring directly to the resolutions passed by the Security Council and published on its website....
2. **On constant basis** verify the customer database and any information received concerning potential or current customers....
3. **Immediately report** to the Regulator in the case of Freezing Funds for the Regulator to report to the Office within five working days from the date of notifying it
4. **Report to the Office**, through the Regulator, if it finds that one of its previous customers
5. **Report to the Office**, through the Regulator, that no action has been taken due to similarity in names
6. **Cancel the Freezing** within five working days from the date of cancelling



Administrative and Penal Measures

Article (20)

1. The Regulator shall undertake all the measures to ensure compliance by financial institutions and designated non-financial businesses and professions with the Relevant Security Council Resolutions and
2. A person, acting in good faith, shall be discharged from administrative liability for damage or from a claim arising from
3. A person who has access to or who, directly or indirectly, by reason of his position, becomes aware of any information
4. A person who violates the obligations provided for in this Resolution shall be punished by the criminal and administrative penalties



Date: 1 May 2019

Notice No.: FSRA/FCPU/13/2019

To: Senior Executive Officers (SEO), Money Laundering Reporting Officers (MLRO) and Principal Representatives (PR) of Relevant Persons

Dear SEO/MLRO/PR,

RE: Cabinet Resolution No. 20 of 2019

The UAE Cabinet have passed Resolution No. 20 of 2019 Concerning the Regulation of Terrorism lists and the application of the Security Council resolutions and the relevant resolutions on the prevention, suppression of terrorism and its financing and the cessation of weapon proliferation and its financing (hereon referred to as 'the Resolution').

On 15 April 2019, the Financial Crime Prevention Unit (FCPU) held discussions with the relevant federal authorities concerning the Resolution and implementation steps. During the discussions, the importance of the implementation of the Resolution was emphasized as it is part of the preparations for the upcoming FATF Assessment to enhance our regulatory framework, especially in relation to international cooperation.

What is required from Relevant Persons?

All relevant authorities have been instructed to cross-check their clients databases, and require their regulated entities to do so, against the sanctions list available at the following link: <https://www.un.org/securitycouncil/content/un-sc-consolidated-list>

Where a positive match is identified, then a written response must be sent to the FCPU no later than 13 May 2019. **No response is required if your search results in negative matches, (i.e. Nil).**

All Relevant Persons are reminded to verify and cross-check their client database and any information received concerning potential or current clients to the Sanctions List on an ongoing basis.

Administrative and Penal Measures

Relevant Persons are reminded to ensure that they meet the required obligation as failure to do so may result in the FSRA imposing penalties. These obligations are explained most notably in the AML Rulebook under Sections 11 ("SANCTIONS AND OTHER INTERNATIONAL OBLIGATIONS"). Furthermore, disregarding the required obligations may result in criminal penalties provided for in the Federal Decree by Law No. 20 of 2018.

Sincerely

FINANCIAL CRIME PREVENTION UNIT

Update on the GoAML

03

A decorative graphic at the bottom of the slide consisting of numerous thin, white, wavy lines that create a textured, ocean-like effect. The lines are arranged in a series of parallel, undulating bands that span the width of the slide.



What is “goAML system”

- FIU’s new reporting system;
- All reporting entities in UAE are required to register on the goAML platform in order to submit suspicious reports. By completing the registration on FIU’s new reporting platform
- ADGM is administering an instruction from a Federal level and thus mandatory compliance is required.
- AML requirement applicable to all Relevant Persons under ADGM.

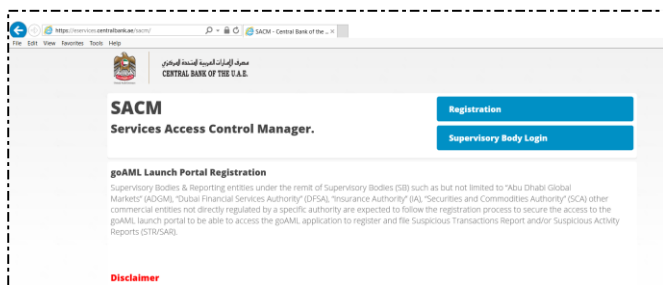
How to register on “goAML”



- Register on goAML

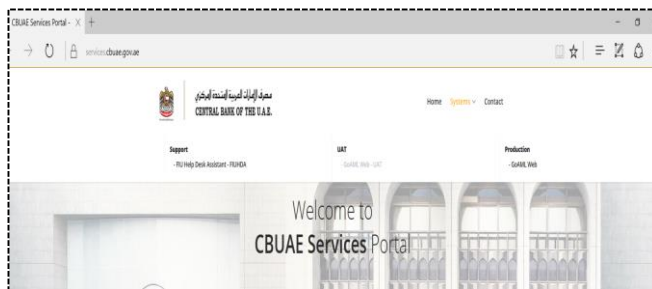
1. Pre-registration (Service Access Control Manager)

<https://eservices.centralbank.ae/sacm/>



2. UAE goAML (Anti-Money-Laundering System)

<https://services.cbuae.gov.ae/>





Required documents/attachment for “goAML”

FIs	DNFBPs	RegLab
<ul style="list-style-type: none">Financial Service Permission (FSP)Supporting evidence of the current MLRO and deputy MLRO (i.e. copies of passport, UAE Resident Visa and UAE ID).The ADGM Recognized Person Status Form	<ul style="list-style-type: none">ADGM Registration LicenseSupporting evidence of the current MLRO (i.e. copies of passport, UAE Resident Visa and UAE ID).	<ul style="list-style-type: none">Financial Service Permission (FSP)Supporting evidence of the current MLRO and deputy MLRO (i.e. copies of passport)

Hints:

- **Mobile number**
 - Valid and working UAE Mobile number
- **Swift code**
 - Only to be used by reporting entities which are financial institutions. Others can input N/A

Update on the goAML statistics



Update as 13 October 2019								
Stages	Preregistration			Overall	goAML Registration			Overall
Types	FIs	DNFBPs	RegLab		FIs	DNFBPs	RegLab	
Approved or Activated	55/62	73/112	12/19	140/193	51/62	55/112	8/19	113/193
Not Register/connected	7/62	39/112	7/19	53/193	11/62	57/112	11/19	79/193

- kindly contact goAML team goaml@cbufae.gov.ae; or goAML support team on 02 691 5407 to help you in case if you face any technical issue.
- The survey link: <https://services.cbufae.gov.ae/>

Thematic review

04

A decorative graphic at the bottom of the page consisting of multiple thin, white, wavy lines that create a textured, undulating effect across the width of the slide.

By Email

29 September 2019

Ref.: ADGM-19-0068L-CEO

To: Senior Executive Officers (SEOs), Money Laundering Reporting Officers (MLROs) and Principal Representatives (PRs) of Authorised Persons

Dear All,

FINDINGS OF THE AML THEMATIC REVIEW AND NEXT STEPS

During March and April 2019 the Financial Services Regulatory Authority ("FSRA") conducted a thematic review ("the Review") of the practices of Authorised Persons ("APs") in ADGM in relation to preventing and detecting the acts of money laundering, terrorist financing and the financing of weapons of mass destruction¹. This letter provides an overview of the findings from the Review, which comprised a desk-based analysis of the annual AML Returns received from forty-two APs and the on-site inspection of nine of them, and important messages arising from it that should be considered by APs.

BACKGROUND

The Review focused on the following three key matters.

1. The Risk Based Approach ("RBA")
2. Customer Due Diligence ("CDD")
3. Sanctions monitoring

The Review was designed and undertaken to allow the FSRA to assess the effectiveness of the systems and controls being used by APs in order to comply with the obligations imposed on them by the ADGM AML Rulebook. Based on the findings of the Review and the insights gained from it, the FSRA has identified a number of areas where current practices are effective in reducing those risk types, but also a number of areas where APs can improve their practices and by doing so enhance their systems and controls, further reducing those risk types within ADGM.

FINDINGS

In general, the findings revealed that the majority of APs have taken appropriate measures to implement the required systems and controls as prescribed in our AML Rulebook. However, there were

¹ For the purposes of this letter the term "risk types" will be used to cover the risks to an AP arising from these acts and the term "anti-money laundering" ("AML") will be used to refer collectively to the actions undertaken to counter those activities and the associated risks.

FINANCIAL SERVICES REGULATORY AUTHORITY
سلطة تنظيم الخدمات المالية

Abu Dhabi Global Market Square, Al Maryah Island, PO Box 111999, Abu Dhabi, United Arab Emirates. T +971 2 333 8888
مقرعة سوق أبوظبي العالمي، جزيرة الماريه، ص.ب 111999، أبوظبي، الإمارات العربية المتحدة. هاتف 971 2 333 8888

adgm.com

some shortcomings that must be addressed, as highlighted in more detail below.

1. Application of the Risk Based Approach (RBA)

In some cases business risk assessments, i.e. the analysis undertaken by an AP of its own exposure to these risk types, were not sufficiently detailed to provide any meaningful assistance in formulating a robust AML framework, comprising appropriate systems and controls, for the AP. Furthermore, these assessments were not always reviewed and updated on a regular basis. The FSRA also observed that in a number of cases generic risk managements reports were produced which did not specifically address these risk types arising from the specific nature of the business, customers, products and services of the AP.

2. Customer Due Diligence (CDD)

The FSRA noted a number of shortcomings in the performance of CDD, both whilst onboarding new customers but also on an ongoing basis in accordance with the risk rating determined for each customer. Certain APs were unable to specify the type of CDD undertaken as well as the frequency of conducting ongoing CDD for customers commensurate with their respective customer risk ratings (i.e. based on categorization as High, Medium or Low). It was also noted that some APs failed to carry out ongoing CDD. In the instances where ongoing CDD was conducted, certain APs were unable to identify the specific sections in their policies and procedures that specified how they should undertake CDD.

3. Sanctions Monitoring

Customers were generally screened against the relevant sanctions lists, both international and those drawn up by the UAE authorities ("local"), when they were on-boarded and thereafter, but some APs could not provide an indication of the frequency with which post-onboarding screenings were performed. It is unclear whether sanctions screenings were performed when triggers are met or whether the screening was carried out on a periodic basis. Thus, the FSRA concluded that sanctions compliance for some APs was regarded as an ad hoc activity rather than being treated as a core regulatory process. In cases where APs are relying on technological platforms offered by various service providers, they must ensure that appropriate mechanisms are in place to monitor these platforms' accuracy in order meet the APs obligations in sanctions monitoring.

Additionally, some APs were unable to show that they had screened customers against the relevant UAE sanctions list when it was released/updated or on a periodic basis thereafter.

AREAS FOR IMPROVEMENT AND NEXT STEPS

AML is a key regulatory concern for ADGM, in line with the UAE national efforts to combat financial crime. The annex to this letter contains examples of good practices that were observed during the Review and areas where APs should improve their practices. This can be achieved through strengthening existing systems and controls or adopting new, supplementary processes where necessary.

FINANCIAL SERVICES REGULATORY AUTHORITY
سلطة تنظيم الخدمات المالية

Abu Dhabi Global Market Square, Al Maryah Island, PO Box 111999, Abu Dhabi, United Arab Emirates. T +971 2 333 8888
مقرعة سوق أبوظبي العالمي، جزيرة الماريه، ص.ب 111999، أبوظبي، الإمارات العربية المتحدة. هاتف 971 2 333 8888

adgm.com

Page 7 of 6



The FSRA will continue to monitor industry practices in relation to AML, in order to ensure that high, effective control standards are maintained by APs. Failure to comply fully with the requirements of the Federal AML Laws and ADGM AML Rulebook may result in the imposition of supervisory measures including possible enforcement actions.

The Financial Crime Prevention Unit ("FCPU") of the FSRA will continue to conduct outreach sessions and issue further specific guidance to raise the level of awareness and compliance.

Sincerely,

Richard Teng
Chief Executive Officer

FINANCIAL SERVICES REGULATORY AUTHORITY
سلطة تنظيم الخدمات المالية

Abu Dhabi Global Market Square, Al Maryah Island, PO Box 111999, Abu Dhabi, United Arab Emirates. T +971 2 333 8888
مبنى سوق أبوظبي العالمي، جزيرة الماريه، ص.ب 111999، أبوظبي، الإمارات العربية المتحدة. هاتف +971 2 333 8888

adgm.com



Annex: Good Practices and Areas for Improvement

General
General Remarks
<p>APs should:</p> <ul style="list-style-type: none"> • understand that regulatory requirements are the minimum standards that must be met; • employ appropriate expertise and experience in dealing with AML; • be aware that when outsourcing tasks to another entity, especially in relation to CDD, the ultimate responsibility for meeting regulatory requirements rests with the AP so they must have a detailed knowledge of the related activities undertaken by that entity; • appreciate that AML measures are global in nature, across their operations; and • proactively monitor international standards that are critical in formulating global AML standards (i.e. those from FATF, the UN, the Basel AML index).
1. Application of the Risk Based Approach (RBA)
Good Practices
<p>The Business risk assessment process:</p> <ul style="list-style-type: none"> • uses all available sources of information, e.g. FATF Mutual Evaluations reports and the Basel AML index, to support the identification and analysis of risk types; • engages senior management, business areas and control functions (e.g. compliance, risk management) as part of the review and approval process; and • identifies and considers all key financial crime risks, including tax evasion and corruption.
Areas for Improvement
<p>APs should:</p> <ul style="list-style-type: none"> • ensure that the assessment is an integral part of formulating their AML framework; • use a granular approach to the assessment and document it, rather than assign a headline risk rating without detailed analysis of the underlying risk types; and • assess the effectiveness of various AML controls in the light of the specific, inherent risks that those controls are intended to mitigate.
2. Customer Due Diligence (CDD)
Good Practices
CDD methodology and processes:



<ul style="list-style-type: none"> • are well-documented in an AML Manual that includes a section addressing ongoing CDD and ongoing transaction monitoring, and is written in plain English; • clearly define the client risk rating methodology; • require a central client risk rating register to be established prior to onboarding any customer; and • utilize screening software against lists of key names and entities including customers, beneficial owners and known associates, on an ongoing basis, and generate real time alerts.
<p>Areas for Improvement</p>
<p>APs should:</p> <ul style="list-style-type: none"> • ensure a meaningful differentiation between the classifications of Low, Medium and High risks, with supporting analysis based on the relevant risk factors for those categories; • screen the relevant name(s) (including UBOs) against all relevant sanctions lists at the time of on-boarding and thereafter; • ensure - when onboarding a customer belonging to a group where there is an existing relationship - that customer due diligence requirements are the same as would be applicable to a new customer; • set clear protocols for the frequency of on-going CDD that are appropriate for the different customer risk ratings (whether Low, Medium or High); • conduct searches using a variety of information sources, with a focus on sources of funding and wealth, ownership and organizational structure, composition of senior management, authorized signatories who will act on behalf of the client or their agent; and • review AML policies and procedures on a periodic basis (at least annually) and whenever there is a material change to circumstances, whether internal or external (e.g. new legislation).
<p>3. Sanctions Monitoring</p>
<p>Good Practices</p>
<p>Monitoring:</p> <ul style="list-style-type: none"> • screens customers at the time of onboarding and then periodically, in accordance with the relevant sanctions lists; • utilizes electronic software/solutions to monitor sanctions lists.
<p>Areas for Improvement</p>
<p>APs should:</p> <ul style="list-style-type: none"> • ensure a consistent and documented approach when screening the names of all agents and UBOs against various sanctions lists including the local lists before their onboarding or when establishing a relationship with the client or their agent; • have clear action plans defined for next steps when a “hit” is seen; and • ensure that sanctions lists, both international and local, are monitored and kept up-to-date.

Thank You

