

Guidance

Technical Guidance prior to start filling out and submitting the online AML Return form:

1. Relevant Persons are reminded that all answers are mandatory. The system will not allow any submission in case of any mandatory question marked with an asterisk remaining unanswered.
2. Relevant Persons have the option to save their work in progress at any stage of filling the AML Return form. The related saved file can be accessed for review and amendment prior to submission.
3. **Relevant Persons are reminded that a signed copy of the filled AML Return form is required to be uploaded under 'Signed AML Return' prior to submission.**
4. **Once the AML Return form is fully completed, Relevant Persons should ensure saving the form to allow the 'Download Report' button to appear after the form is saved. Once downloaded, the AML Return form can be printed, signed, and uploaded (refer to point 3 above). If the 'Download Report' button does not appear, it is an indication that there are unpopulated mandatory fields, which once completed and the report is saved, the said button should be visible.**
5. **The AML Return form cannot be edited after submission. Any resubmission will require completing all the questions again.**
6. Text fields allow a maximum of 20k characters, where additional space is needed, Relevant Persons are required to upload the detailed answers separately highlighting for each answer the related question and its number.
7. Relevant Persons should receive a notification on their mailbox confirming that the AML Return for the relevant year was successfully submitted on the date of such submission.

General Guidance while completing the AML Return form:

1. In completing this AML Return, Relevant Persons should refer to the Anti-Money Laundering and Sanctions Rules and Guidance (AML).
2. A Glossary of defined terms is provided in AML Chapter 3.
3. A reference in the AML Return to "Money Laundering" includes a reference to Terrorist Financing (TF), Proliferation Financing (PF), the financing of unlawful organizations and sanctions non-compliance unless the context provides or implies otherwise.
4. All Relevant Persons must complete and submit this AML Return by the end of April each year in accordance with AML 4.6.1. The AML Return must cover the period from 1 January to 31 December of the preceding year (*unless previously authorised by the FSRA*).
5. Relevant Persons must retain a signed copy of the completed AML Return along with all supporting materials (*refer to the above-mentioned Guidance 6*).
6. Separately, a Relevant Person must also report at least semi-annually to its Governing Body or Senior Management on the matters set out in AML 12.4.1. In accordance with AML 12.4.3, copies of these reports and the records made under AML 12.4.2(c) must be submitted to the Relevant Person's ADGM Regulator.
7. For any queries, please reach out to FCCP by email at amlreturn@adgm.com.

1 Core Information

1.1 Details of Relevant Person

Relevant Person's Name

Commercial License or Financial Services Permission Number

Relevant Person's Type

Specify Category (Cat.)

Submission Date

Start of Reporting Period

End of Reporting Period

1.2 Money Laundering Reporting Officer (MLRO)

1.2.1. Name of MLRO

a) Did the MLRO hold any other role(s) with the Relevant Person or its Group during the reporting period?

Please list the role(s)

b) Is the MLRO function outsourced?

i. On average, how many hours per month did the MLRO provide his services to the Relevant Person?

ii. How many entities did the MLRO act for?

c) Has the Relevant Person changed MLRO during the reporting period?

Please provide the reason(s) for the change in MLRO

d) Please specify the MLRO reporting lines/s [AML12.2.1 (a)]

1.2.2. Deputy MLRO

a) Name of Deputy MLRO

1.3 Governance and Oversight

Specify whether the Senior Management or Governing Body were involved in any of the following during the reporting period

Action

Senior Management

Governing Body

a) Approval of the Business Risk Assessment		
b) Discussion on AML risks at Governing Body meetings		
c) Oversight of AML compliance review(s) conducted in accordance with AML 4.1.1(4) and any subsequent remedial action		
d) Review of regular AML compliance reports		
e) Approval of business partners or respondent/correspondent banks		
f) Approval of Politically Exposed Persons (PEPs), higher-risk clients, transactions or products		
g) Approval of policies, procedures or other relevant systems and controls		
h) Influencing decisions regarding Suspicious Activity Reports		
i) Other (specify)		

1.4 Reporting

a) Specify the frequency of the MLRO's internal reports [AML 12.4.1]	
b) Specify to whom the internal reports were circulated	
c) Confirm whether the semi-annual report has been prepared in accordance with AML 12.4.1	
Please provide the reason for not preparing the Semi – Annual Report.	
d) Confirm whether copies of the reports submitted to the Governing Body and Senior Management and the associated assessments made during the reporting period have been submitted to the Regulator in accordance with AML 12.4.3	
Please provide the reason for not submitting the Semi – Annual Report.	

1.5 Business Risk Assessment (BRA)

a) Provide the date of the last BRA undertaken by the Relevant Person [AML 6.1.1]	
b) Did this BRA take into consideration the results of the most recent UAE National Anti-Money Laundering and Terrorist	

Financing Risk Assessment Report?

c) Did the Relevant Person identify and assess Terrorism Financing (TF) and Proliferation Financing (PF) risks for their customers, countries or geographic areas, products, services, transactions, or delivery channels?

d) Did the Relevant Person consider other factors in conducting its BRA?

e) Did the Relevant Person introduce any of the following during the reporting period [AML 6.1.3]

i. New product

ii. New service

iii. New business practice

iv. New or developing technology

i. Did any of these introductions impact the BRA during the reporting period?

ii. Please provide details of the impact of these introductions

f) Is there any type of client, transaction, or product (within the scope of the Relevant Person's commercial license or Financial Services Permission) which the Relevant Person prohibits due to its AML risk appetite?

Please describe these and the reasons why

g) Does the Relevant Person assess the potential risk arising from other financial crimes, such as fraud, theft of personal data and cyber security risks [AML 6.1.3]?

i. Fraud

ii. Theft of personal data

iii. Cyber security risks

iv. Other (specify)

Please describe the process/es in place for this assessment

1.6 Policies, Procedures, Systems and Controls

a) Provide the date of the last review of the effectiveness of the Relevant Person's AML policies, procedures, systems and controls [AML 4.1.1(4) and AML 6.2.1(c)]

b) Specify who the review was undertaken by [AML 4.1.1 (5) and AML 10.4.1] (where applicable)

c) Specify the scope of this review [AML 4.1.1(6)]

d) Provide the date of the last review and update of your AML policy(ies)

e) Does your AML policies, procedures, systems and controls cover Targeted Financial Sanctions (TFS) and Proliferation Finance (PF) measures

1.7 Groups, Branches and Subsidiaries

a) Is the Relevant Person part of a Group [AML 4.2]?

Describe the arrangements in place with Group entities to ensure the appropriate sharing of AML-related information [AML 4.3]

b) Is the Relevant Person an ADGM Entity, with a branch, subsidiary, or a Group entity in the ADGM [AML 4.2]?

Describe the arrangements in place to ensure that its operations comply with its policies, procedures, systems and controls [AML 4.2]

1.8 Sanctions

a) Did the Relevant Person screen all of its customers and transactions against local and international lists?

b) Please specify which lists the Relevant Person screens against:

c) What arrangements did the Relevant Person have in place to comply with relevant resolutions and Sanctions? The response should specify the:

i. Roles involved

ii. Frequency of any screening

iii. Maintenance of lists

iv. Any technology utilised [AML 11.1.1(1)]; Specify the respective name(s) of the service provider(s)

d) Did the Relevant Person rely on an in-house or a third-party technology for sanctions screening?

e) During the reporting period, did the Relevant Person become aware of an event specified under AML 11.1.1(2) that required it to make a report to its Regulator?

Please specify the following information

Sanction Action	Number of Events
Events Identified	
Events Reported to Regulator	
f) Specify the number of Sanctions Screening alerts reviewed during the reporting period	
No. of Payment Sanctions Screening Alerts	
No. of Customer Database Sanctions Screening Sanctions Alerts	
g) Where the Relevant Person relies on third party technology for sanctions screening, please specify the following:	
i. How it has satisfied itself that the technology includes a comprehensive and up-to-date list of resolutions and Sanctions that the Relevant Person must comply with?	
ii. The frequency that the screening lists are updated by the technology provider	
h) Describe the arrangements in place to ensure that the Relevant Person complies with relevant government, regulatory and international findings, resolutions and Sanctions [AML 11.2.1(1)]	
i) Has the Relevant Person subscribed to the website of the Executive Office for Control and Non-Proliferation (EOCN) to receive updates whenever a change is applied on the United Nations Security Council Resolutions and UAE national sanctions lists?	
j) Did the Relevant Person screen the database and transactions on a regular basis against the names listed on the United Nations Security Council Resolutions and UAE national sanctions lists issued under the EOCN website?	
k) Is the Relevant Person aware of the requirement to notify the Supervisory Authority in case of the detection of a positive match?	
l) In the event where the Relevant Person identified a "positive hit" of any designated person or entity, what Targeted Financial Sanctions actions were taken to ensure full compliance with the obligations under Article 21 of Cabinet Decision No.74 of 2020?	
m) When a match is found through the screening process, did the Relevant Person implement freezing measures as well as submitting a reporting without delay through GoAML platform?	
n) Did the Relevant Person maintain records of all screening results (negative, false positive, potential, and confirmed matches) for a period of at least six years?	
o) Is the Relevant Person aware of completing the TFS mandatory survey after each sanction alert notification received by the EOCN?	
p) Does the Relevant Person conduct business involving dual-use goods?	

Did the Relevant Person:

i. Have a clear dual-use goods policy?

ii. Have a screening mechanism for transactions involving dual-use goods?

iii. Update dual-use goods list into its sanctions screening system?

How did the Relevant Person update dual-use goods list into its sanctions screening system?

iv. Review dual-use goods in transactions to ensure that they do not involve weapons of mass destruction?

Detail the standard operating procedure

1.9 Suspicious Activity Reports (SARs) /Suspicious Transactions Reports (STRs) and Other Types of Reports on the goAML

a) Has the Relevant Person registered on the UAE Financial Intelligence Unit's (FIU) goAML system?

b) Have all external SARs / STRs been submitted to the UAE FIU via the goAML system?

c) Specify the number of SARs / STRs reported during the reporting period [AML 14.2.2 and AML 14.3.1(c)]

SAR / STR Type

Total Number of SARs / STRs

i. Internal (to MLRO)

ii. External (to UAE Financial Intelligence Unit through the goAML)

Reason for Reporting (external SARs/STRs)

Reporting Number

d) Does the Relevant Person consider raising STR/SARs through the goAML for Rejected or Terminated cases ?

i.Specify the number of SAR/STRs raised through the goAML for prospective customers Rejected:

Reason for Rejection

Number of Related Rejections

	Money Laundering	Terrorism Financing	Proliferation Financing
Providing fake / forged / inaccurate / mismatching documents			
Identifying mismatch in selfie and ID			
Providing incorrect / invalid / unclear ID or Selfie			
Breaching signed policy / contract			
Refusing / reluctant to provide adequate KYC information / documents			
Lack of required supporting information and documents			
Unclear / Unjustified / Unverified Source of Fund / Source of Wealth			
Unsatisfactory CDD/EDD for a trigger event / adverse media			
Relation outside the Relevant Person's risk appetite			
UNSC Sanctions			
UAE Sanctions			
Other economic sanctions (OFAC, EU, etc)			
FATF jurisdictions subject to a Call for Action ("Blacklist")			
Other (Specify)			
Total SAR/STRs for cases Rejected			

ii.Specify the number of prospective customers rejected without raising SAR/STRs to the FIU through the goAML:

Reason for Rejection

Number of Related Rejections

Reason for not raising SAR/STRs to the FIU

Providing fake / forged / inaccurate / mismatching documents		
Identifying mismatch in selfie and ID		
Providing incorrect / invalid / unclear ID or Selfie		
Breaching signed policy / contract		
Refusing / reluctant to provide adequate KYC information / documents		
Lack of required supporting information and documents		
Unclear / Unjustified / Unverified Source of Fund / Source of Wealth		
Unsatisfactory CDD/EDD for a trigger event / adverse media		
Relation outside the Relevant Person's risk appetite		
UNSC Sanctions		
UAE Sanctions		
Other economic sanctions (OFAC, EU, etc)		
FATF jurisdictions subject to a Call for Action ("Blacklist")		
Other (Specify)		

Total Cases Rejected Without Filing SAR/STRs

iii. Specify the number of SAR/STRs raised through the goAML for existing customer's relations Terminated:

Reason for Termination	Number of Related Terminations		
		Money Laundering	Terrorism Financing
			Proliferation Financing

Providing fake / forged / inaccurate / mismatching documents			
Identifying mismatch in selfie and ID			
Providing incorrect / invalid / unclear ID or Selfie			
Breaching signed policy / contract			
Refusing / reluctant to provide adequate KYC information / documents			
Lack of required supporting information and documents			
Unclear / Unjustified / Unverified Source of Fund / Source of Wealth			
Unsatisfactory CDD/EDD for a trigger event / adverse media			
Unsatisfactory CDD/EDD for transaction monitoring alerts e.g., Deviation in transactions' behaviour / unjustified and repeated 3rd party payments etc			
Unrealistic / high value of invoices not in line with the client's business activity			
Relation / Transactions outside the Relevant Person's risk appetite			
UNSC Sanctions			
UAE Sanctions			
Other economic sanctions (OFAC, EU, etc)			
FATF jurisdictions subject to a Call for Action ("Blacklist")			
Other (Specify)			

Total SAR/STRs for cases Terminated

--	--	--

iv. Specify the number of existing customer's relations terminated without raising SAR/STRs to the FIU through the goAML:

--

Reason for Termination

Number of Related Terminations

Reason for not raising SAR/STRs to the FIU

Providing fake / forged / inaccurate / mismatching documents		
Identifying mismatch in selfie and ID		
Providing incorrect / invalid / unclear ID or Selfie		
Breaching signed policy / contract		
Refusing / reluctant to provide adequate KYC information / documents		
Lack of required supporting information and documents		
Unclear / Unjustified / Unverified Source of Fund / Source of Wealth		
Unsatisfactory CDD/EDD for a trigger event / adverse media		
Unsatisfactory CDD/EDD for transaction monitoring alerts e.g., Deviation in transactions' behaviour / unjustified and repeated 3rd party payments etc		
Unrealistic / high value of invoices not in line with the client's business activity		
Relation / Transactions outside the Relevant Person's risk appetite		
UNSC Sanctions		
UAE Sanctions		
Other economic sanctions (OFAC, EU, etc)		
FATF jurisdictions subject to a Call for Action ("Blacklist")		
Other (Specify)		

Total cases Terminated without filing SAR/STRs

--	--

e) Has the Relevant Person notified the Regulator of SARs /STRs reported to the UAE FIU?

--

f) Where applicable, did the Relevant Person submit the dedicated report for cash and / or wire transfers transactions exceeding the set threshold ('Dealers in Precious Metals and Stones Report ("DPMSR")' and 'Real Estate Activity Report ("REAR")')? [AML 8.1.1(5)].

1.10 Training

a) List the AML/CFT and TFS training, conferences and events attended by the MLRO and Deputy MLRO, where applicable, during the reporting period

MLRO

Training's Number

Training's Details

Deputy MLRO

Training's Number

Training's Details

b) Did the relevant Person conduct adequate internal training and awareness on AML obligations and sanctions evasion typologies to relevant staff and senior management?

Specify below the number of relevant Employees that completed AML training during the reporting period

Role	Number Completed	Number Not Completed
Senior Management & Government Body		
Client Facing Employees		
Risk, Compliance & Internal Audit		
Operations (Finance, IT, HR, administration etc)		
Other (specify)		

c) Did Relevant Person conduct adequate internal training and awareness on TFS (TF & PF) obligations and typologies to relevant staff and senior management?

Specify below the number of relevant Employees that completed TFS (Proliferation and Terrorism Financing) training during the reporting period:

Role	Number Completed	Number Not Completed
Senior Management & Government Body		

Client Facing Employees		
Risk, Compliance & Internal Audit		
Operations (Finance, IT, HR, administration etc)		
Other (specify)		

d) Where relevant Employees did not complete training during the reporting period, what were the reasons for this?

e) Specify when the Relevant Person provided AML and Sanctions trainings to relevant Employees during the reporting period:

Specify the scope of topics covered in the training material:

f) Specify how the training was provided:

1.11 Notifications

a) Has an event occurred requiring the Relevant Person to notify the Regulator under the AML Rules? [AML 4.1.2, 4.4.1, 4.4.2]

Specify the date/s of this/these notification/s and the event/s that occurred

2 Supplementary Information

2.1. Customer Risk Assessments (CRAs)

a) Specify from which channels the Relevant Person accepted new customers

b) Describe the process for conducting CRAs including the roles involved and any technology or templates utilised

c) For non-face-to-face customers, please specify the below

i. The roles involved

ii. Did the Relevant Person have process in place for conducting e-KYC CRAs?

Provide details about the process in place

iii. Did the Relevant Person have any technology utilized for e-KYC?

Please specify the respective name(s) of technology utilized?

iv. Did the Relevant Person adopt measures to mitigate e-KYC risks [AML 8.3 Guidance]?

Provide details about these measures

d) Provide an overview of the Relevant Person's CRA methodology including the prescribed customer risk ratings, associated due diligence levels and frequency of reviews

e) Describe the onboarding procedure in place and illustrate how the Relevant Person adopts a risk-based approach when dealing with customers

f) Describe the CDD conducted during the onboarding process, including the roles involved and any technology or templates utilised [AML 8.1 to 8.2]

g) What measures did the Relevant Person have in place to ensure that a consistent level of CDD is undertaken for each client type (individual, body corporate, partnership, trust etc) relative to their risk rating [AML 8.3 to 8.5]

h) For non-face to face customers, did the Relevant Person combine e-KYC with transaction monitoring, anti-fraud and cyber-security measures to support a wider framework preventing applicable Financial Crime

i) Describe the process for conducting ongoing CDD, including the roles involved and any technology or templates utilised. Please specify whether this process differs depending on the customer's risk profile [AML 8.6]

j) Specify how customer data is maintained by the Relevant Person

k) Specify the location of the Relevant Person's customer data

l) Specify whether the Relevant Person's transaction monitoring process is

m) If the Relevant Person's transaction monitoring is "automated", specify the technology used

n) If the Relevant Person's transaction monitoring is "manual", please describe the related process

o) Specify the number of transaction monitoring alerts reviewed during the reporting period

p) Is any of the transaction monitoring alerts reviewed during the reporting period related to cases of fraud or theft of personal data?

Specify the number

q) Did the Relevant Person have in place arrangements to comply with the Decision of the National Committee for Combating Money Laundering and Financing Terrorism and Illegal Organizations (the Committee) regarding FATF High-Risk Jurisdictions?

Specify what arrangement did the Relevant Person have in place to

comply with this Decision?

r) Did the Relevant Person apply enhanced CDD measures to all business relationships and transactions with FATF high-risk jurisdictions?

s) Does the Relevant Person report to Financial Intelligence Unit ("FIU") any transactions involving natural persons or legal entities from FATF high-risk jurisdictions before conducting such transactions?

t) What is the number of transactions involving natural persons or legal entities from FATF high-risk jurisdictions reported to the FIU?

2.2. Reliance and Outsourcing

a) Did the Relevant Person rely on a third party "qualified professional" to conduct one or more elements of CDD on its behalf?

Please list these below [AML 9.1.1(1)]

Name of Qualified Professional	Type of Qualified Professional (e.g. financial institution, group entity, law firm etc)	Element/s of CDD undertaken (e.g. collection of documentation, data entry, due diligence checks etc)

b) Describe the arrangements in place to ensure that the Relevant Person has access to the CDD information from the third party, in compliance with AML 9.1.1(3)(a) and (b)

c) Did the Relevant Person have an outsourcing agreement in place with the third party that complies with GEN 3.3.32 [AML 9.3.1]?

2.3. Business Partner Identification

a) Did the Relevant Person have a process for conducting Business Partner identification including the roles involved and any approvals sought [AML 9.2.1]

i. Describe the Relevant Person's process for conducting Business Partner identification including the roles involved and any approvals sought [AML 9.2.1]

ii) How frequently is the ongoing due diligence on Business Partners undertaken?

--

2.4. Employee Screening

Did the Relevant Person screen employees to ensure high standards when hiring employees depending on their nature, size and level of complexity? [AML 12.3.1 Guidance]

--

What is the process for conducting such a screening:

i. Method adopted:

--

ii. Screening list(s):

--

iii. Tool(s):

--

iv. Frequency of such screening:

--

3 Correspondent Banking and Wire Transfers

3.1. Correspondent Banking

a) Did the Authorised Person conduct any correspondent banking activities with a respondent bank?

--

b) Is the Authorised Person satisfied that the respondent bank undertook CDD at least equivalent to that in AML 8.3.1 in respect of its customers who were party to the correspondent banking relationship and this information is available upon the Authorised Person's request [AML 10.2.1(g)]?

--

c) Has the Authorised Person maintained records to demonstrate compliance with the requirements in AML 10.2.1?

--

3.2. Wire Transfers

a) Did the Authorised Person send or receive funds by wire transfer on behalf of a customer [AML 10.3.2]?

--

i) Did the Authorised Person screen all of the originators and beneficiaries of these wire transfers?

--

ii) Did the Authorised Person screen other details in these wire transfers?

--

Provide details about the fields screened

iii) Specify whether all completed wire transfers contained:

• accurate originator and beneficiary information [AML 10.3.2(1)(a)]?

• the minimum information specified in AML 10.3.2(3)?

iv) Describe the process for screening wire transfers including the roles involved, any technology used and the policy for rejecting or suspending wire transfers

4 Customers and Transactions Data

For Fund Managers, the term "Customer" should be understood as referring to "Unit Holders"

As at the end of the reporting period

4.1. Breakdown of customers by nationality (for natural persons) or domicile (for non-natural persons)

Geographical Area	Number of Customers which are natural persons	Number of Customers which are non-natural
UAE		
GCC (other than UAE)		
Middle East (other than UAE & GCC)		
Africa		
Asia		
Oceania		
North America		
South America		
Europe and UK		

Overall Total Number of Customers

--	--

4.2 Breakdown of customers by residency status (for natural persons)

Geographical Area	Number of Customers which are natural persons	Specify the country (ies)
UAE		
GCC (other than UAE)		
Middle East (other than UAE & GCC)		
Africa		
Asia		
Oceania		
North America		
South America		
Europe and UK		
Overall Total Number of Customers		

4.3 Breakdown for customers which are non-natural

Legal Persons	Legal Arrangements	Type of Legal Arrangements
Overall Total Number of Customers		

4.4 Breakdown of customers from FATF high risk and other monitored jurisdictions

FATF Jurisdiction	Number of Customers
-------------------	---------------------

--	--

Overall Total Number of Customers

--

4.5 Breakdown of customers by risk rating

Risk Rating

Number of Customers

--	--

Overall Total Number of Customers

--

4.6 Breakdown of customers by type of due diligence

Number of Standardised due diligence

Number of Enhanced due diligence

Overall Total Number of due diligence

--	--	--

4.7 Customers and beneficial owners identified as PEPs [AML 8.3 Guidance]

PEP Type

Number of Customers

Nationality

Number of Beneficial
Owners

Nationality

a) Domestic (UAE)

--

--

--

--

b) Foreign

--

--

--

--

4.8 Breakdown of customers by status

Customer Status

Internal Definition of Status

Number of Customer

Active

--

--

Inactive

--

--

Dormant

Overall Total Number of Customers

4.9 Cash Transactions

Does the Relevant Person accept cash transactions:

Specify:

i. The total number of cash transactions processed

ii. The total amount (aed) of cash transactions processed

5 Declaration

5.1. I declare that, to the best of my knowledge and belief, having made due enquiry, the information given in this return is complete and correct.

5.2. I understand that under ADGM's:

- a. Financial Services and Markets Regulations 2015, section 219, it is an offence to mislead the Regulator by knowingly or recklessly providing to the FSRA any information which is false, misleading, or deceptive or to conceal information where the concealment of such information is likely to mislead or deceive the FSRA; and
- b. Commercial Licensing regulations 2015, section 39(4), it is a contravention of the Regulations to knowingly or recklessly provide false or misleading information to the Registrar, in a material particular.

5.3. I understand that any personal data provided to the ADGM will be used to discharge its regulatory functions under the Abu Dhabi Law No. 4 of 2013 and other relevant legislation and may be disclosed to third parties for those purposes only.

5.4. I confirm that I have the authority to complete this form, to declare as specified above and sign this form for, or on behalf of, the Relevant person.

Name of the person filling this AML Return

Function of the person filling this AML Return

Emirates ID Number

Uploaded File Names