[ZONE]

AML, CTF and SANCTIONS

Policy and Controls

Policy Reference No.	
Version	
Date of Update	
Approved By	
Chief Compliance Officer	**Lana Pebley** **l.pebley@rakez.com** **+971 2041133**

Contents

Introduction

The Zone and its directors and other senior management are committed to carrying out the Zone's activities in compliance with all applicable laws, rules and regulations and to maintaining the highest ethical standards in relation to its business activities.

This document sets out the Zone's anti-money laundering ("**AML**"), countering terrorist financing ("**CTF**") and sanctions compliance policies, controls and procedures and provides guidance on how to recognise and deal with red flags and associated risks.

The policies and procedures in this document apply to the Zone and its subsidiaries. All employees, officers and directors are required to adhere to these standards in order to protect the Zone and its reputation in relation to money laundering, terrorist financing and sanctions related risks.

AML AND CTF COMPLIANCE POLICY

INTRODUCTION

The Zone is committed to complying with all laws, rules and regulations relating to anti-money laundering ("**AML**") and counter terrorism financing ("**CTF"**) applicable to its business and operations.

The Zone does not conduct or permit any person to use the Zone to conduct illegal activity. The Zone will therefore not register or license any entity where customer due diligence ("**CDD**") cannot be satisfactorily completed, or where there is knowledge or reasonable grounds to suspect that the entity/applicant is engaged in money laundering or terrorist financing.

The Zone has established and maintains AML/CTF procedures, systems and controls to prevent and detect money laundering and terrorist financing, which ensure compliance with UAE Federal laws and take into consideration international best practice.

All employees, officers and directors of the Zone (collectively, "**Employees**"), as well as consultants, representatives, agents, brokers, distributors, and other intermediaries must comply fully with this policy and the accompanying procedures when they are acting on behalf of the Zone.

WHAT IS MONEY LAUNDERING?

Money laundering is the process by which those involved in criminal activities conceal the source and disguise the nature of illicit funds by making them appear legitimate.

Under the laws of the UAE, money laundering can arise from property derived from the following offences: crimes involving narcotics and psychotropic substances; kidnapping, piracy and terrorism; breaches of environmental laws; illicit dealing in fire-arms and ammunition; bribery; embezzlement and damage to public property; fraud; breach of trust and related offences; tax evasion; regulatory breaches; insider dealing; and any other related offence referred to in international conventions to which the UAE is a party.

The process generally involves three stages:

- **Placement**, where the money launderer introduces the proceeds of crime into the financial system. This is the point when proceeds of crime are most at risk of detection;
- **Layering**, where the money launderer engages in transactions, conversions or movements of the funds to distance them from their source. Detection can be difficult at this stage; and

- **Integration**, when the money launderer has disguised the proceeds of crime, the funds can re-enter the legitimate economy. This is the most difficult stage of money laundering to detect.

In the context of our business, money laundering might involve the following (below is a non-exhaustive list of examples):

- Company formation as part of a complex trust and company structure to layer funds or hide their true criminal origin;
- Company formation in a free zone to hide the identity of businesses engaged in illegal activity; and
- Nominee shareholders used to hide the identity of the true business owners.

WHAT IS TERRORIST FINANCING?

Terrorist organisations may seek to raise funds through legitimate sources, including through abuse of charitable entities or legitimate businesses through criminal activity, or from state sponsors and activities in failed states and other safe havens. This may be in small amounts.

A single terrorist organisation may use a number of different financing methods. However, the sources of terrorist financing can be divided into two general types:

- **financing from above**, in which large-scale financial support is aggregated centrally by states, companies, charities or permissive financial institutions; and
- **financing from below**, in which terrorist fundraising is small-scale and dispersed, for example based on self-financing by the terrorists themselves using employment income or welfare payments.

Terrorist financing is closely related to money laundering and international efforts to locate and cut off the funding of terrorist financing are broadly aligned with efforts in respect of money laundering. Therefore, where this document refers to "money laundering", this is to be considered to include terrorist financing.

KEY REQUIREMENTS

Broadly speaking, there are two key AML and CFT requirements:

- Conducting CDD by collecting relevant information and records on Zone entities/applicants (and keeping such records up to date) including any person who is applying for or renewing a registration or licence in the Zone (collectively "**Clients**").

- Identifying and reporting any knowledge or suspicion of money laundering (as described further in the procedures). If you come across any transaction or activity which you believe is suspicious, in that you think it may involve money derived from criminal activities or may be related to terrorism financing, the details must be reported to the Chief Compliance Officer immediately.

In addition, Employees are strictly prohibited from:

- Making or becoming involved in any payment connected to or transferring anything of value that you know or suspect is derived from, criminal activity.

- Engaging in any activity that may involve money laundering or terrorist financing. For example, false invoicing practices, bribery and corruption and otherwise assisting others in concealing the sources of money derived from criminal activity, or in creating the impression that illegally derived money or other assets were legitimately obtained.

- Providing funds to a terrorist or a terrorist organisation, intending that the funds will be used for terrorism or terrorism-related crimes.

PENALTIES FOR NON-COMPLIANCE

Compliance with this policy and the accompanying procedures by all Employees, regardless of their role or location, is mandatory.

Failure to comply with AML and CFT laws may expose the Zone and individual Employees to significant business losses, reputational harm and/or civil and criminal liability. A breach of this policy and/or the accompanying procedures may lead to (a) disciplinary action, including dismissal or termination of employment for gross misconduct, and/or (b) referral to appropriate law enforcement officials in the UAE or third countries. The Zone reserves the right to take any additional action as it, in its sole discretion, deems appropriate to secure the diligent and proper implementation and enforcement of this Policy.

ROLE OF THE CHIEF COMPLIANCE OFFICER

The Zone has appointed a Chief Compliance Officer (“Compliance Officer”) who is the custodian of this policy, responsible for maintaining the Zone's AML/CTF procedures, systems and controls.

The Compliance Officer is of sufficient seniority to act on his/her own authority and has a direct line of communication to senior management and the board of directors of the Zone.

The Compliance Officer is the Zone's point of contact for the relevant UAE authorities and is responsible for promptly responding to any request for Compliance related information from the UAE Central Bank or other appropriate bodies.

The Compliance Officer will be provided with sufficient resources to undertake his/her role, including relevant employees within the Zone's compliance function whose role is to assist the Compliance Officer, including the execution of duties in an effective, objective and independent manner.

The Compliance Officer acts as the point of contact for employees concerning money laundering matters and receives internal suspicious transactions reports, undertakes investigations of any report received and, where the Compliance Officer in their sole discretion thinks necessary, reports suspicions to the relevant UAE and other authorities.

The Compliance Officer is responsible for reporting relevant matters related to money laundering to the Zone's board of directors on an annual basis and conducting a risk assessment in relation to the Zone's AML and CTF controls.

The Compliance Officer acts as an education resource for all employees of the Zone and is responsible for establishing and maintaining an appropriate anti-money laundering training programme. The Compliance Officer also puts in place adequate awareness arrangements and provide employees with periodic and *ad hoc* information regarding money laundering and updates employees on findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions issued by the government of the UAE (or any government department in the UAE), the Central Bank of the UAE or the AMLSCU and UAE enforcement agencies concerning names of persons, groups, organisations or entities or any other body where suspicion of money laundering or terrorist financing exists. The Compliance Officer also keeps up-to-date with relevant money laundering trends, rules and regulations and undertakes external training where appropriate.

* * *

SANCTIONS COMPLIANCE POLICY

INTRODUCTION

It is the policy of the Zone to fully comply with all sanctions laws and regulations of the United Arab Emirates, United Nations, United States and European Union (including the United Kingdom), as well as other such laws and regulations, when applicable to its business (collectively, "**Sanctions**").

The Zone shall not register or license any entity that is, to the best of our knowledge, designated, or whose shareholders[1], beneficial owners, directors or managers are designated as targets of Sanctions. In addition, the Zone shall not conduct, or allow Clients to use the Zone to conduct business with any individual, entity, country or territory that is a target of Sanctions unless the Zone has first ensured that such business complies with applicable law and does not involve any sanctionable activity.

All Zone Employees, as well as consultants, representatives, agents, brokers, distributors, and other intermediaries when they are acting on behalf of the Zones, shall comply fully with these requirements.

It is the Zone's policy to respect, uphold and comply with all Sanctions applicable to our business.

The Zone will not register or license any company or person designated as a Sanctions target.

The Zone will also not participate in transactions designed or intended to evade applicable Sanctions.

All Employees must ensure that the transactions in which they are involved on behalf of the Zones comply will all applicable Sanctions.

Compliance with this Policy by all Employees, regardless of their role or location, is essential. Failure to comply with applicable Sanctions laws may expose the Zones and individual Employees to significant business losses, reputational harm and/or civil and criminal liability. Lack of compliance with this Sanctions Policy by Employees may also result in disciplinary action, including termination of employment.

[1] Shareholder is an individual, group or organization that owns one or more shares in a company, and in whose name a share certificate is issued, and, for the purposes of this Policy, shareholders refer to direct/immediate shareholders

Specific Policy Requirements:

1. **General Requirement –** The Zone shall not register or license any company that is designated, or whose shareholders, beneficial owners, directors or managers are designated as targets of Sanctions. The Zone shall collect sufficient background information from applicants at the time of registration, and shall refresh this information at the time of license renewal, to determine if they are ineligible for registration or renewal based on this standard or if they are otherwise high-risk under Sanctions (*e.g.,* due to operations in or ownership by persons located in Iran or Syria). In addition, the Zone will not conduct, or allow the use of the Zone to conduct, any business with or involving any individual, entity, vessel, country or territory which is a target of Sanctions imposed by the United Arab Emirates, United Nations, United States, European Union (including the United Kingdom), or other applicable jurisdiction ("**Sanctions Targets**"), unless the Compliance Department ("**Compliance**") shall have first ensured that such business complies with applicable law and does not otherwise expose the Zone to Sanctions risk.

2. **Embargoed Territories –** Embargoed Territories are, at present, **Crimea**, **Cuba**, **Iran**, **North Korea** and **Syria**. The Zone shall not license any company, or otherwise allow any company to operate in the Zone, if that company or its shareholders, beneficial owners, managers and/or directors are resident, registered or incorporated in an Embargoed Country. In addition, the Zone shall not allow the use of the Zone to conduct any business involving an Embargoed Territory unless such business does not involve US Persons (*defined below*), US territory, the US financial system and/or exports of US-origin goods (collectively, "**US Elements**") and complies with all other applicable Sanctions requirements (as confirmed by Compliance). The Zone shall have zero tolerance for any sanctionable activity by persons operating in the Zone.

3. **Screening –** The Sanctions authorities of the United Arab Emirates, United Nations, United States, European Union (including the United Kingdom) and other relevant jurisdictions maintain extensive lists of Sanctions Targets. Before licensing any new Clients to operate in the Zone, renewing a registration or engaging in significant transactions with introducers or other agents or counterparties, appropriate due diligence must be undertaken and the names of the Clients, their shareholders, beneficial owners, directors and managers must be screened to determine whether they are a target of UAE, UN, US, EU, UK or other applicable Sanctions or whether their transactions with or through the Zones may involve an Embargoed Territory. All screening matches must be referred to Compliance for review. No licenses, renewals or transactions shall be processed until Compliance has completed its assessment of the screening match.

4. **Payments –** Even if otherwise permitted under this Policy, (i) payments involving an Embargoed Territory or other US Sanctions Target must not be made in USD; (ii) payments involving an EU Sanctions Target must not be made in EUR; and (iii) payments involving UAE Sanctions targets are prohibited.

5. **US Persons –** "US Persons" include anyone while physically present in the United States; any US citizen or green card holder, wherever located (including dual nationals of the US and another

country); any US-incorporated entity, or anyone employed by a US entity. US Persons must not participate in any transaction involving an Embargoed Territory or other US Sanctions Target. Please refer to the ***US Person Insulation Policy*** set out in **Appendix 1**.

6. **EU Persons –** "EU Persons" include anyone while in the territory of the European Union; any national of an EU Member State, wherever located; any EU-incorporated entity, or, for the purposes of this policy, anyone employed by an EU-incorporated entity. Please refer to the ***EU Person Recusal Policy*** set out in **Appendix 2**.

7. **Transparency –** The Zone will not knowingly assist any third party in breaching the law, or participate in any criminal, fraudulent or corrupt practice in any country. Full transparency with the Zone's banks and counterparties is required in relation to any transaction involving Embargoed Territories or Sanctions targets, even after Compliance has confirmed that such transaction complies with all applicable Sanctions.

8. **Training and Guidance –** Relevant employees will receive appropriate training and guidance in relation to Sanctions issues. Employees should consult Compliance whenever they have any Sanctions-related questions or concerns.

Behaviour that is in breach of the law or this policy must be reported to a supervisor or manager.

Further Sanctions compliance procedures may apply to your transactions. In cases of doubt, you must consult the Compliance Officer.

* * *

AML, CTF AND SANCTIONS COMPLIANCE PROCEDURES

1. CUSTOMER DUE DILIGENCE ("CDD")

All persons with or for whom the Zone proposes to form a business relationship or undertake transactions (*i.e.,* Clients), including licensing, incorporation or registration,[2] must be subject to CDD in accordance with these procedures prior to effecting any business with that Client.

The Zone adopts a "**risk-based**" approach to CDD whereby all new and existing Clients are risk-assessed at the time of on-boarding or other submissions (such as requests for licence renewal) and the CDD process, including sanctions screening and risk assessment, is updated/refreshed whenever there are changes to a Client's profile (*e.g.,* change in ownership or directors/managers).

The CDD required depends on the type of person with whom the Zone proposes to form a business relationship or undertake transactions as well as other factors which might affect the money laundering/terrorist financing or sanctions risk presented by a person. In all situations, the objective is to obtain satisfactory evidence of that person's true identity, as well as the purpose of the relationship.

Step 1 – Conduct Standard CDD

For all applicants/Clients seeking to incorporate or license an entity/establishment in the Zone, Sales team will first complete the questionnaire attached at **Appendix 3** and obtain the following information:

1. The proposed entity/establishment type (*e.g.,* free zone or non-free zone).
2. The proposed name of the entity.
3. The proposed entity's registered address and principal place of business.[3]
4. The proposed entity's licence type (*e.g.,* commercial, industrial, general trading, etc.)
5. The intended purpose and nature of the business activities of the entity (and confirmation that the entity does not engage in "**Prohibited Activities**"). ***A generic***

[2] Forming a company is treated as forming a business relationship even if the formation of the company is the only transaction carried out for that Client. This is due to the potential risk involved in facilitating the formation of a company structure that may be abused by a Client.

[3] An entity's principal place of business includes the country of the entity's main operating office.

***business activity description (such as "management services" or "general trading") is not sufficient*.**

6. Full name, local (*if any*) and home country address, date of birth, and nationality(-ies) (including all nationalities held) of all proposed **directors/ senior managers**, as well as, in each case, the following documents:

   (a) ***evidence of identity*** (current, signed passport or current, signed ID card or other official *government issued* identification documentation that is customary in the country of residence, including a clear picture, the individual's full name, date and place of birth and nationality);

   In addition, for each director which is a corporate entity, obtain:

   (a) the full name of the corporate entity, its registration number and registered address and principal place of business;

   (b) ***the constitutional documents of the corporate:***

   - Certificate of incorporation or registration;
   - Any trade licence or equivalent;
   - Current articles of association and memorandum of association;
   - Current certificate of incumbency or certificate of good standing or Register of Extracts, as applicable;
   - Passport copy of authorised signatories; and
   - The full name, local (*if any*) and home country address, date of birth, and nationality(-ies) (including all nationalities held) of all shareholders and Beneficial Owners.

7. Full name, local (*if any*) and home country address, date of birth, and nationality(-ies) (including all nationalities held) of all **Beneficial Owners**, as well as in each case, ***evidence of identity*** (current, signed passport or current, signed ID card or other official *government issued* identification documentation that is customary in the country of residence, including a clear picture, the individual's full name, date and place of birth and nationality).

"**Beneficial owners**" are individuals who ultimately own or control the entity, or on whose behalf a transaction or activity takes places. For a company, a beneficial owner is any individual who:

- owns or controls at least 25% of the shares or voting rights;
- ultimately owns or controls whether directly or indirectly at least 25% of the shares or voting rights in the business;
- holds the right, directly or indirectly, to appoint or remove a majority of the board of directors;
- has the right to exercise, or actually exercises, significant influence or control over the corporate body;
- exercises ultimate control over the management; or
- controls the corporate body.

If shares or rights are held by a nominee, the beneficial owner will be the person for whom the nominee is acting. If the nominee is acting for a legal entity, then the beneficial owner will be the person who exercises ultimate control over the legal entity.

For a ***partnership***, a beneficial owner is any individual who controls more than 25% of the capital of the partnership, or who ultimately is entitled to control more than 25% of the voting rights of the partnership.

For a ***trust***, a beneficial owner includes: the settlor, trustees, beneficiaries and any individual who has control over a trust.

Where the immediate owners/shareholders of the entity are not individuals (or where they are acting on behalf of a third party), the above information must be obtained for the individuals who are the Beneficial Owners.

8. Full name, local (if any) and home country address, date of birth, and nationality(-ies) (including all nationalities held) of any individual acting on behalf of the entity pursuant to a Power of Attorney or by other means, as well as evidence of identity (such as a current, signed passport or current, signed ID card or other official government issued identification documentation that is customary in the country of residence, including a clear picture, the individual's full name, date and place of birth and nationality);

9. Valid copy of the Power of Attorney, legally attested by a relevant authority (as applicable).

10. Sanctions Policy Questionnaire (please refer to Appendix 7)

11. Any other document required by the Company Regulations

Foreign Language Documents

If documents are in a foreign language, you must satisfy yourself that they do in fact provide evidence of the entity/individual's identity.

1.1 **Step 2 – Conduct Initial Compliance Checks**

On the basis of the information and documents obtained as part of the Standard CDD process, following compliance checks will be conducted:

- Conduct screening using an external compliance screening database (Accuity, WorldCheck, LexisNexis or equivalent) of the full names of the Client and its Beneficial Owners, directors/senior managers and power of attorney holders;

- Review the Client's registered address, as well as home country address information, nationality(-ies) of the Client's Beneficial Owners, directors/senior managers and power of attorney holders for reference to an Embargoed Territory; and

For the assessment of address information, Compliance should consider both the city and country of residence and registration or incorporation. This is particularly important for Clients, Beneficial Owners, directors/senior managers and power of attorney holders that are resident, registered or incorporated in Russia or the Ukraine where confirmation is needed that these individuals and/or companies are not based in Crimea.

a) Determine whether the Client has any exposure to Embargoed Territories by reviewing the information collected in the Sanctions Exposure Questionnaire and information in the Appendix 3.

These compliance checks will address the following matters:

- Sanctions (including potential connections with Embargoed Territories through the Sanctions Questionnaire).

- Identification of politically exposed persons ("**PEPs**") and close family members, associated persons (see box below on definition of PEPs).

- Adverse media related to AML, CFT or Sanctions issues.

No licenses, renewals or transactions shall be processed until these checks have been completed.

Compliance checks will be documented by completing the relevant questions in **Appendix 3** and including these materials in the Client file.

If the CDD materials obtained in Step 1 do not contain sufficient information to allow the completion of the checklist and questionnaire, further information will be collected from the Client.

The compliance checks will be conducted on a maker/checker (*i.e.,* four-eye) basis. If the maker and checker do not reach the same conclusion regarding the (a) disposition (*i.e.,* whether the potential match is a "*true*" match) of the results generated through the screening system searches, (b) the assessment of the address information for the Client and its Beneficial Owners, directors/senior managers and power of attorney holders and/or (c) the assessment of information collected about the Client's principal place of business and exposure to the Embargoed Territories, the file will be referred to the Compliance Officer who will make the final decision.

1.2 **Step 3 – Conduct Risk Assessment/Rating**

On the basis of the information and documents provided as part of Steps 1 and 2, risk assessment will be conducted to rate the Client as either "High Risk" or "Standard Risk".

The following Clients are to be classified as "High Risk" (*i.e.,* are high risk Clients, or "**HRC**"), and subject to the enhanced due diligence procedures at Step 4 below:

No.	High Risk Factors
1	All Clients where one or more Beneficial Owners, directors, senior managers or power of attorney holders are listed as a Sanctions Target by the Central Bank of the UAE, UN, US and/or the EU (including the UK).
2	All Clients with potential links to Embargoed Territories (*i.e.,* **Crimea**, **Cuba**, **Iran**, **North Korea** and **Syria**). This applies in the following circumstances (among others): Any director, senior manager, Beneficial Owner, Power of Attorney holder has an address in, or is a national of an Embargoed Territory. ➢ The Client is owned or controlled by the Government of an Embargoed Territory; ➢ The Client has business involving, directly or indirectly, an Embargoed Territory (*e.g.,* sales or purchases, including through intermediaries or trans-shipments); or

No.	High Risk Factors
	➢ The Client has operations in an Embargoed Territory (subsidiaries/branches/joint ventures). ➢ In addition, all Clients owned or controlled by, or operating as agents of the Government of Venezuela.
3	An Accuity search or equivalent indicates that the Client or its Beneficial Owner(s) is a PEP, immediate family of a PEP or a close associate of a PEP. Certain types of persons can also pose a greater risk of money laundering, including "**Politically Exposed Persons**" or "**PEPs**" who may wish to use their business relationship with the Zones as a medium for laundering money obtained by way of corruption. PEPs include individuals who are or have been entrusted with prominent public functions in a country or territory, for example • heads of state or of government, • senior politicians (including members of parliaments or equivalent legislative bodies), • senior government, judicial or military officials and ambassadors, • senior executives of state-owned co-operations, • important political party officials (*e.g.* members of the governing body), • senior individuals within international organisations such as the UN or NATO, but not middle ranking or more junior individuals in these categories. A person is a PEP while they hold such a function or position and for at least 12 months after they cease to hold such a function or position. All former PEPs are to be escalated to the Compliance Officer who, at their discretion, will apply a risk based approach to determine whether the former PEP status represents a risk and requires EDD. Close associates of PEPs are persons who have (i) joint ownership with a PEP of a legal entity or arrangement; (ii) any other close business relationship with a PEP; or (ii) sole Beneficial Ownership of a legal entity or arrangement set up for the benefit of a PEP.

No.	High Risk Factors
4	The Client undertakes High Risk business activity: • Dealing in bitcoin and other cryptocurrencies • Aviation services • Lending activities • Charities or non-for-profit organisations • Coins investment and trading • Activities in defence industry • Debt collection agencies • Money Service Businesses • Insurance activities (not including brokers and agents) • Dealers in precious metals and stones • High value/luxury goods dealers • Trusts • Mining • Energy
5	A shareholder, director, senior manager, Beneficial Owner, power of attorney holder is resident, registered or incorporated in a **high-risk country**. For guidance on High Risk Countries – see the **High Risk Countries Matrix** at **Appendix 4.**
6	Other factors are present which indicate increased risk (*i.e.,* all Clients/applicants in relation to which red flags are identified as presenting a higher risk of money laundering, that have not been satisfactorily addressed). For guidance on High Risk Factors – see the **Red Flag Guidance** at **Appendix 5.**

1.3 **Step 4 – Conduct Enhanced Due Diligence (for HRCs)**

Enhanced Due Diligence ("**EDD**") applies in situations that are higher risk. This means taking additional measures to examine the background and purpose of a relationship or transaction and applying additional measures, as outlined below.

The extent of enhanced due diligence is at the absolute discretion of the Compliance Officer who will agree on a range of additional measures, and may include one or more of the following.

- For entities with directors, senior managers, Beneficial Owners or Power of Attorney holders who are nationals of an Embargoed Territory, it is required to verify that the individual is not resident in an Embargoed Territory by requesting a valid UAE residency permit and two of the following:

a. Copy of a utility bill (2 months);

b. Copy of a bank account statement (2 months); and

c. Copy of a rental/lease agreement or title/mortgage/deed to property.

- identification and verification of the full ownership structure;
- analysis of any complex structures including the use of trusts or multiple jurisdictions (in which case the Zone seeks to establish that any such structures are bona fide by reference to their stated legal purpose);
- additional documentary evidence such as secondary proof of identity or an additional proof of address, or verification of the identity of directors/managers/Beneficial Owners through independent sources;
- requesting that copies of Clients' documentation are certified by a bank, financial institution, lawyer or notary who are competent at document inspection, or a person from a regulated industry or in a position of trust;
- obtaining a legal and certified translation of documents in a foreign language;
- taking supplementary measures to verify the documents received (for example, checking them against additional independent sources), and potentially meeting face-to-face with the Client (if not yet not done) or initiating telephone contact with the Client or their representative;
- further analysis of proposed business activities, including reviewing a business plan for higher risk Clients;
- taking more steps to understand the history, ownership and financial standing of the parties;
- obtaining audited financial statements;
- obtaining evidence of source of wealth (income, assets, net worth etc.) – ***this is mandatory for all Clients associated with PEPs***;
- obtaining evidence of source of funds, such as a bank statement, reference or introductory letter - ***this is mandatory for all Clients associated with PEPs***;
- obtaining confirmation of employment and/or compensation;
- seeking written undertakings from the Client that they will comply with applicable laws and will notify the Zone of suspicious activity; and
- for Clients with potential links to Embargoed Countries, it may be appropriate to conduct the Sanctions specific desktop EDD measures listed below:

a) Reviewing the information on the "About Us," "Where we Operate," "Our Locations," and "Contact Us" (or the equivalent) sections of the Client's website for references to an Embargoed Territory;

b) Reviewing the first page of results returned by the following Google searches: (i) [Client main name] + Crimea; (ii) [Client main name] + Cuba; (iii) [Client main name] + Iran; (iv) [Client main name] + North Korea; (v) [Client main name] + Syria;

c) *If there is a search function available on the Client's website*, reviewing the results returned by the following searches: (i) Crimea; (ii) Cuba; (iii) Iran; (iv) North Korea; and (v) Syria; and

d) For Clients that do not have a website and/or are owned by another company, also conduct the same steps (*i.e.,* (b) – (d)) for the Beneficial Owner, or, if necessary, the owner's owner.

1.4 **Step 5 – Approval/Refusal**

No HRC can be on-boarded without approval of the Compliance Officer. The Compliance Officer and/or the business has the right to escalate any case to the Zones' Compliance Committee for a decision in relation to on-boarding/approval. Rationale for the decision to on-board an HRC must be maintained on file.

For RAK Maritime City, approval of HRCs is the responsibility of the Zone Manager and the Compliance Officer.

Compliance Committee

Ras Al Khaimah ("RAK") Zones' Compliance Committee is a governance body established by the Board of the Investment and Development Office to oversee the implementation of the Compliance Programme at each of the Zones.

The RAK Compliance Committee will review requests escalated by the Zones to reject, approve, or continue to provide services to HRCs in cases where the Zones' Compliance Committee or the Compliance Officer deem it appropriate and necessary.

The rationale for the decision to on-board a Client must be maintained on file.

The Zone shall not approve, register or license any entity in the following categories:

- Where CDD cannot be completed satisfactorily.
- Where the Client is a listed Sanctions Target.

- Where any of the Client's Beneficial Owners, directors/senior managers or power of attorney holders are listed Sanctions Targets.
- Where the Client or any of its Beneficial Owners, directors/senior managers or power of attorney holders is (a) resident, registered or incorporated in an Embargoed Territory; or (b) owned or controlled by, or operating as agents of, the Government of an Embargoed Territory or the Government of Venezuela.
- Where the Zone considers in its absolute discretion that the Client presents unacceptable reputational risk to the Zone.
- Where the Zone considers in its absolute discretion that the Client is outside the Zones' risk appetite.
- Where the Client is or is owned by a bearer share corporation or shell bank.
- Where the Client (or its Beneficial Owners or directors/senior managers) are: (i) wanted by Interpol; (ii) wanted by international authorities for organized crime-related offenses; and (iii) accused (within the past 7 years) or wanted by international authorities for money-laundering or terrorism-related crimes.
- Where the Client is engaged in **prohibited business** activities:

  a) Gambling and gambling related activities

  b) Any other activity that is contrary to local law or the public policies of the Emirate

All HRC applicants with connections to Embargoed Countries, if on-boarded and as a condition of on-boarding (or upon identifying such connection), are to sign the following representation:

> *"We confirm that all of our business with, through or involving [insert name of the Zone] will not involve a sanctioned country (at present, Crimea, Cuba, Iran North Korea or Syria), including goods procured from or transhipped through a sanctioned country, or violate or cause [insert name of the Zone] to violate any economic or financial sanctions or trade embargoes implemented, administered or enforced by the United Arab Emirates, the United Nations, United States, European Union, United Kingdom or other relevant sanctions authorities."*

Any deviation from the above requirements can only be authorised by the Compliance Officer and /or Compliance Committee at the request of the Zones or Compliance Officer with full documentation and explanation as to risk mitigation related to acceptance of such Client to ensure compliance with all applicable laws, regulations and Sanctions.

1.5 **Step 6 – Data recording and Ongoing Screening**

Information collected as part of the CDD process is recorded in an electronic database (*i.e.,* SAP/Sales Force); as follows:

- Full name of the Client
- Full name, local (*if any*) and home country address, including country of residence, registration or incorporation, nationality and country of passport(s) held (*if relevant*) of all:

  (a) individuals who are Beneficial Owners;

  (b) directors/senior managers; and

  (c) power of attorney holders.

Information will be entered into SAP/Sales Force on a maker/checker (*i.e.,* four-eye) basis to ensure accuracy.

The database also should include a description of the Client's business, including whether the Client has exposure to the Embargoed Territories or other Sanctions Targets.

All of this data should be stored electronically in a format that is easily searchable.

This information shall be subject to regular and ongoing screening (using the screening solution provided by Accuity) on a daily basis against updates to the official sanctions-related lists administered by the UAE, US and the EU (including the UK) to detect the possible addition of a Client or associated persons to a Sanctions list. In addition, when the local and home country address, nationality and country of passport(s) held fields in SAP/Sales Force are updated, these fields should be screened against a set of geographic search terms for the Embargoed Territories.

1.6 **Step 7 – Periodic Reviews/ Renewals**

Renewals

Core CDD information should be reviewed and refreshed as part of the licence renewal process.

This involves checking that all documents remain active/current. In addition, the compliance checks, risk-rating process and, *where applicable*, EDD described at **Steps 1-4** above must be reviewed and (as necessary and at the discretion of the Compliance Officer) repeated as part of renewal process.

Other Changes

CDD, the compliance checks, risk-rating and, *where applicable*, EDD must also be repeated/refreshed whenever the Zone suspects that information previously obtained is no longer reliable or adequate. If at any time an Employee becomes aware that the Zone lacks sufficient information or documentation concerning a person's identification or develops a concern about the accuracy of current information or documentation, they must inform the Compliance Officer and the Zone will promptly obtain appropriate material to verify the person's identity.

Clients are instructed to notify the Zone of any changes in the registrant's shareholders or directors/managers so that the Zone can update the CDD information. Any change to directors, managers, shareholders or Beneficial Owners of an entity must be subject to CDD as outlined in section 1.1 above.

1.7 Reliance on Third Parties

The Zone may in certain circumstances, rely on third parties to conduct some elements of CDD measures for a Client. The Zone remains fully responsible for the proper conduct of CDD and ongoing monitoring (see section 3 below).

The Zone will enter into an arrangement with such third party/agent allowing the Zone to obtain immediately on request copies of the CDD information from the third party and ensure that the third party retains copies of the CDD information for five years from the date on which the transaction occurs or the business relationship with the Client ends.

1.8 Record Keeping

Copies of the evidence obtained to satisfy CDD is kept for a period of five years from the date on which the business relationship with the Zone comes to an end (for example, the date of expiration/termination of a lease/licence/registration).

1.9 CLIENT EXIT PROCEDURES

Where CDD cannot be completed satisfactorily, including in regard to the Beneficial Ownership of the Client, the Zone will make every reasonable effort to terminate any existing business relationship, will not provide a service to or for the Client, will not establish a business relationship (including issuing a licence or incorporating a Client) or carry out an occasional transaction with the Client and may consider making a suspicious transaction report.

2. REPORTING SUSPICIOUS ACTIVITY

2.1 Requirement to Report

If you suspect, know or have reasonable grounds for knowing or suspecting that money laundering, terrorist financing or a breach of sanctions is or might be taking place, this must be reported to the Compliance Officer without delay.

Suspicious activity reporting will not result in penalties under any circumstances or be reflected negatively in performance reviews.

Reports can be made by email or telephone to the Compliance Officer. Employees should not make disclosures to any government authority, third party or regulatory body (*i.e.,* the AMLSCU) of suspicions of money laundering as all suspicious activity reports should first be evaluated by the Compliance Officer.

Employees must not say or do anything that may prejudice an investigation or suggest to a third party including the Client that a suspicion has been raised, a suspicious activity report has been submitted or that a money laundering or terrorism financing investigation may be carried out (see section 2.5 on "Tipping Off"). Employees must not falsify, modify, conceal or destroy documents relevant to investigations by the Compliance Officer.

The Compliance Officer will make and maintain a record of the report and actions taken.

2.2 **What is suspicious activity?**

Suspicion may arise in a number of different circumstances and may occur prior to establishing a business relationship with a party as well as at a result of that party's behaviour during the establishment of the relationship or at any time thereafter.

Here are some warning signs of potentially suspicious activity. This is not an exhaustive list, and these signs are not always suspicious. It depends on the circumstances of each case.

- checking the Client's identity is difficult
- the Client is reluctant to provide details of their identity or provides fake documents
- the Client is trying to use intermediaries to protect their identity or hide their involvement
- the Client has no apparent reason for using the Zone
- part or full settlement in cash or foreign currency, with weak reasons
- the Client can't give a proper explanation of where money came from
- a third party, apparently unconnected with the Client, bears the costs, or otherwise pays for the service
- an unusually big cash or foreign currency transaction
- the Client won't disclose the source of the funds
- unusual source of funds or unexpected movement of funds into a company

Other factors may indicate suspicion. See further, the **Red Flag Guidance** at **Appendix 5.**

Employees should not reveal the fact that a suspicion has been reported and neither the suspected party nor other colleagues should be informed. Employees are permitted (but not required) in the first instance to discuss suspicions with their line managers when determining whether an internal suspicious transaction report should be made. Employees do not require the permission of their line manager to report a suspicion, and if in doubt, a report should be made to the Compliance Officer.

2.3 **External suspicious transaction reporting**

The Compliance Officer is responsible for investigating any internal suspicious transaction reports made by Employees. The Compliance Officer is authorised to make external reports to appropriate authorities on suspicious activity. The Compliance Officer's investigations may or may not involve engaging employees in further discussion of the suspicions raised. If the Compliance Officer comes to the conclusion that the internal suspicious transaction report gives reason to suspect money laundering, terrorist financing or financial crime, the Compliance Officer independently (and not subject to the consent or approval of any other person) files an external suspicious transaction report with the AMLSCU or other relevant authorities. Employees may or may not be informed that an external suspicious transaction report has been filed.

2.4 **Record keeping requirements**

The Compliance Officer makes written records of steps undertaken to investigate the circumstances in relation to which an internal suspicious transaction report is made and, where the Compliance Officer determines that an external suspicious transaction report should not be made, makes written records of the reasons why. These records and records of any internal suspicious transaction reports and/or external suspicious transaction reports are kept for a period of six years from the date on which the investigation was undertaken/report was made.

2.5 **"Tipping-off"**

It is an offence under Federal Law No. 4 of 2002 for an Employee who knows or suspects or, has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering, not to report the knowledge or suspicion as soon as is reasonably practical after the information came to the employee's attention. In addition, the Zone may take disciplinary action against an Employee for failure to make such a report. Reporting suspicions to the Compliance Officer discharges the Employee's responsibility to report his/her suspicions.

The Zone must not participate in any transaction where they suspect money laundering. However, it is also an offence for anyone to prejudice an investigation into money laundering by disclosing, or "tipping off" to a person under suspicion, or any third party, any information or other matter likely to prejudice an investigation.

Employees should be careful not to inadvertently tip-off a person that they are being scrutinised for possible involvement in suspicious money laundering operations, or that a suspicious activity report has been filed, or that any other competent authority is investigating that person's possible involvement in money laundering operations. This may be difficult where business relations are time critical and require action prior to an external suspicious transaction report being made by the Compliance Officer or where the Compliance Officer is waiting for instructions from the AMLSCU on how to proceed. In such cases, Employees should seek guidance from the Compliance Officer who will immediately contact the AMLSCU for instructions on how to proceed.

3. **REFERRAL PARTNERS / AGENTS**

RAKEZ:

There are three potential types of referral partners/agents used by the Zone: (i) a “Referral Partner”, (ii) an "Introduction Only Agent" and (iii) a "Super Agent".

- A “Referral Partner” is used only for introducing potential Clients to the Zone in exchange for commission. Thereafter the Zone conducts CDD in accordance with the procedures set out above, including on-boarding the Client if a decision is taken to approve the Client.

- An "Introduction Only Agent" is used only for introducing potential Clients to the Zone in consideration of a commission. Such agents assist their clients with the application process and have access to a RAKEZ clients’ portal which allows them to upload Clients’ KYC documentation. Thereafter the Zone conducts CDD in accordance with the procedures set out above, including on-boarding the Client if a decision is taken to approve the Client.

- A "Super Agent" is a company that specializes in the formation of FTZ and onshore companies, as well as the license renewal process for existing Clients. Such agents are used for introducing potential Clients to the Zone in consideration of a commission. Such agents assist their clients with the application process and assist in relation to the license renewal process. Thereafter the Zone conducts CDD in accordance with the procedures set out above, including on-boarding the Client if a decision is taken to approve the Client.

The procedures in this section apply with respect to such "**Agents**".

In all cases, the Zone remains responsible for verifying the CDD performed by an Agent and determining whether to approve the Client for on-boarding. All information provided by the Agent is subject to review and assessment by the Zone prior to on-boarding.

Reliance on CDD performed by Agents

The Zone will, independently and without reliance upon due diligence conducted by Agents, and based upon documents, information and analysis it carries out as required by this Policy, make its own decision to license, register, incorporate or renew licenses for their Clients.

In relation to each new Agent, the Zone will conduct CDD as follows:

3.1 **Step 1 – Collection of CDD Information on Agent**

Before a business relationship is formed with an Agent, the Zone will carry out due diligence and compliance verification processes on the Agent as detailed below, obtaining the following information:

1. Letter of Application to be an approved agent;

2. Full name and registration number of the Agent;

3. The Agent's registered address and principal place of business[4];

4. Full name, local (*if any*) and home country address, date of birth, and nationality(-ies) (including all nationalities held) of all **directors/ senior managers** of the Agent, as well as, in each case, ***evidence of identity*** (current, signed passport or current, signed ID card or other official *government issued* identification documentation that is customary in the country of residence, including a clear picture, the individual's full name, date and place of birth and nationality);

5. Full name, local (*if any*) and home country address, date of birth, and nationality(-ies) (including all nationalities held) of all **Beneficial Owners** of the Agent, as well as in each case, ***evidence of identity*** (current, signed passport or current, signed ID card or other official *government issued* identification documentation that is customary in the country of residence, including a clear picture, the individual's full name, date and place of birth and nationality).

   Where the immediate owners/shareholders of the entity are not individuals (or where they are acting on behalf of a third party), the above information must be obtained for the individuals who are the Beneficial Owners;

[4] An entity's principal place of business includes the country of the entity's main operating office.

6. Business Plan;

7. Copy of Professional Licence in the UAE & Tenancy/Lease contract for UAE office;

8. Copy of AML, CTF and Sanctions Policies and procedures of the Agent;

9. Undertaking that AML, CTF and Sanctions Policies and Procedures are commensurate with this Policy;

10. Acknowledgement of receipt and understanding of the Policy;

11. Non-Disclosure Agreement; and

12. Sanctions Policy Questionnaire (please refer to Appendix 7)

RAK ICC

The Zone does not interact directly with Clients, but rather on-boards them through registered agents.

The Zone conducts CDD of its registered Agents at the time of on-boarding as well as when the registered Agents notifies the Zone of changed partners, key staff and/or compliance officers.

CDD performed by the Agent is then subject to independent compliance verification by the Zone.

Reliance on CDD performed by Agents

The Zone will, independently and without reliance upon due diligence conducted by Agents, and based upon documents, information and analysis it carries out as required by this Policy, make its own decision to license, register, incorporate or renew licenses for their Clients.

For each Client introduced by an Agent, the Agent will sign a Confirmation Letter recording details of all information obtained and signed by the Agent, together with underlying/supporting records.

In all cases, the Zone remains responsible for verifying the CDD performed by an Agent and determining whether to approve the Client for on-boarding. All information provided by the Agent is subject to review and assessment by the Zone prior to on-boarding.

In relation to each new Agent, the Zone must conduct CDD as follows:

3.2 **Step 1 – Collection of CDD Information on Agent**

Before a business relationship is formed with an Agent, the Zone will carry out due diligence and compliance verification processes on the Agent as detailed below, obtaining the following information:

1. Letter of Application to be an approved agent;

2. Full name and registration number of the Agent;

3. The Agent's registered address and principal place of business[5];

4. Full name, local (*if any*) and home country address, date of birth, and nationality(-ies) (including all nationalities held) of all **directors/ senior managers** of the Agent, as well as, in each case, the following documents:

(a) CV of each director/senior manager;

(b) ***evidence of identity*** (current, signed passport or current, signed ID card or other official *government issued* identification documentation that is customary in the country of residence, including a clear picture, the individual's full name, date and place of birth and nationality); and

5. Full name, local (*if any*) and home country address, date of birth, and nationality(-ies) (including all nationalities held) of all **Beneficial Owners** of the Agent, as well as in each case, the following documents:

(a) ***evidence of identity*** (current, signed passport or current, signed ID card or other official *government issued* identification documentation that is customary in the country of residence, including a clear picture, the individual's full name, date and place of birth and nationality).

6. Where the immediate owners/shareholders of the entity are not individuals (or where they are acting on behalf of a third party), the above information must be obtained for the individuals who are the Beneficial Owners.

7. In addition, for each direct shareholder of the Agent which is a corporate entity, obtain:

(a) the full name of the corporate entity, its registration number and registered address and principal place of business;

[5] An entity's principal place of business includes the country of the entity's main operating office and other countries that generate more than 10% of the entity's total annual revenues globally.

(b) The full name, local (*if any*) and home country address, date of birth, and nationality(-ies) (including all nationalities held) of all directors/other significant controllers.

8. Company HR organizational chart;
9. Business Plan;
10. Copy of Professional Licence in the UAE & Tenancy/Lease contract for UAE office;
11. Copy of AML, CTF and Sanctions Policies and procedures of the Agent;
12. Undertaking that AML, CTF and Sanctions Policies and Procedures are commensurate with this Policy;
13. Acknowledgement of receipt and understanding of the Policy;
14. Sanctions Policy Questionnaire (please refer to Appendix 7);
15. Non-Disclosure Agreement; and
16. Name and details of compliance officers of the Agent, including CV.

Foreign Language Documents

If documents are in a foreign language, you must satisfy yourself that they do in fact provide evidence of the entity/individual's identity.

3.3 **Step 2 – Conduct Initial Compliance Checks on Agent**

On the basis of the information and documents obtained as part of the Standard CDD process, following compliance checks will be conducted:

- Conduct screening, using an external compliance screening database (Accuity, WorldCheck, LexisNexis or equivalent) (of the full names of the Agent and its Beneficial Owners, directors/senior managers and power of attorney holders;

- Review the Agent's registered address, as well as home country address information, and nationality(-ies) of the Agent's Beneficial Owners, directors/senior managers and power of attorney holders for reference to an Embargoed Territory;

- Determine whether the Agent has any exposure to Embargoed Territories by reviewing the information collected about the Agent's principal place of business in Appendix 6;

- Company internal HR structure chart for the Agent is reviewed to ensure that the structure within the organisation is fit for purpose;

- CVs of partners and key staff are requested along with visa page or employment contract in order to verify if they are employed by the agency; and

- Onsite inspection of the Agent is carried out to ensure that the office is manned as per the organization chart and they have facilities to maintain the book of accounts for all companies under their management. Whereas the Compliance Officer has absolute discretion as to the frequency of such inspections for individual Agents, the Zones must carry out no less than one inspection in a four-year period.

No Agent can be on-boarded until these checks have been completed.

Compliance checks will be documenting by completing the relevant questions in **Appendix 6** and including these materials in the Agent file.

If the CDD materials obtained do not contain sufficient information to allow to the completion of the checklist and questionnaire, further information will be collected from the Agent.

Compliance screening will be conducted on a maker/checker (*i.e.,* four-eye) basis. If the maker and checker do not reach the same conclusion regarding the (a) disposition (*i.e.,* whether the potential match is a "*true*" match) of the results generated through the screening system, (b) the assessment of the address information for the Client and its Beneficial Owners, directors/senior managers and power of attorney holders and (c) the assessment of information collected about the Client's principal place of business and exposure to the Embargoed Territories, the file will be referred to the Compliance Officer, who will make the final decision.

The Zone will send each Agent a link to this compliance policy and require the Agents to confirm by reply email that they have read the policy and will maintain policies and procedures sufficient to ensure that they do not introduce any entity to the Zone in violation of the Zone's policy requirements.

3.4 **Step 3 – Agent Risk Assessment/Rating**

On the basis of the information and documents provided as part of the CDD above, risk assessment will be conducted to rate the Agent as either "High Risk" or "Standard Risk".

The following Agents are to be classified as "High Risk" and subject to the enhanced due diligence procedures at Step 4 below:

No.	High Risk Factors
1	All Agents where one or more Beneficial Owners, directors, senior managers or power of attorney holders are listed as a Sanctions Target by the Central Bank of the UAE, US and/or the EU (including the UK).
2	All Agents with potential links to Embargoed Territories (*i.e.,* **Crimea**, **Cuba**, **Iran**, **North Korea** and **Syria**). This applies in the following circumstances (among others): Any director, senior manager, Beneficial Owner, power of attorney holder has an address in, or is a national of an Embargoed Territory. ➢ The Agent is owned or controlled by the Government of an Embargoed Territory; ➢ The Agent has business involving, directly or indirectly, an Embargoed Territory; or ➢ In addition, all Agents owned or controlled by, or operating as agents of the Government of Venezuela.
3	An Accuity search or equivalent indicates that the Agent or its Beneficial Owner(s) is a PEP, immediate family of a PEP or a close associate of a PEP. See section 1.3 for further guidance
4	A director, senior manager, Beneficial Owner is resident, registered or incorporated in a **high-risk country**. For guidance on High Risk Countries – see the **High Risk Countries Matrix** at **Appendix 4.**

No.	High Risk Factors
5	Other factors are present which indicate increased risk (*i.e.,* all Agents in relation to which red flags are identified as presenting a higher risk of money laundering, that have not been satisfactorily addressed). For guidance on High Risk Factors – see the **Red Flag Guidance** at **Appendix 5.**

3.5 **Step 4 – Enhanced Due Diligence (for High Risk Agents)**

Enhanced Due Diligence ("**EDD**") applies in situations that are higher risk. This means taking additional measures to examine the background and purpose of a relationship or transaction and applying additional measures, as outlined below.

The extent of enhanced due diligence is at the absolute discretion of the Compliance Officer who will agree on a range of additional measures, and may include one or more of the following.

- For Agents with directors, senior managers, Beneficial Owners or Power of Attorney holders who are nationals of an Embargoed Territory, it is required to verify that the individual is not resident in an Embargoed Territory by requesting a valid UAE residency permit and two of the following:

    a) Copy of a utility bill (2 months);

    b) Copy of a bank account statement (2 months); and

    c) Copy of a rental/lease agreement or title/mortgage/deed to property.

- identification and verification of the full ownership structure;

- compliance audit by a reputable audit firm, requested at the Compliance Officer's discretion, to confirm that the Agent has implemented a compliance policy in line with the standards of this Policy, and that the Agent applies CDD procedures no less extensive and effective than those set out in these operating procedures;

- analysis of any complex structures including the use of trusts or multiple jurisdictions (in which case the Zone seeks to establish that any such structures are bona fide by reference to their stated legal purpose);

- additional documentary evidence such as secondary proof of identity or an additional proof of address, or verification of the identity of directors/managers/Beneficial Owners through independent sources;

- taking supplementary measures to verify the documents received (for example, checking them against additional independent sources), and potentially meeting face-to-face with the Agent (if not yet not done) or initiating telephone contact with the Client or their representative;

- further analysis of proposed business activities including reviewing a business plan for higher risk Agents;

- analysis of any complex structures including the use of trusts or multiple jurisdictions (in which case the Zone seeks to establish that any such structures are bona fide by reference to their stated legal purpose), obtaining a structure chart showing the ownership structure of the entity;

- taking more steps to understand the history, ownership and financial standing of the parties;

- obtaining audited financial statements;

- obtaining evidence of source of wealth (income, assets, net worth etc.);

- obtaining confirmation of employment and/or compensation;

- seeking written undertakings from the Agent that they will comply with applicable laws and will notify the Zone of suspicious activity; and

- for Agents with potential links to Embargoed Countries, it may be appropriate to conduct the Sanctions specific desktop EDD measures listed below:

    a) Reviewing the information on the "About Us," "Where we Operate," "Our Locations," and "Contact Us" (or the equivalent) sections of the Client's website for references to an Embargoed Territory;

    b) Reviewing the first page of results returned by the following Google searches: (i) [Client main name] + Crimea; (ii) [Client main name] + Cuba; (iii) [Client main name] + Iran; (iv) [Client main name] + North Korea; (v) [Client main name] + Syria;

    c) If there is a search function available on the Client's website, reviewing the results returned by the following searches: (i) Crimea; (ii) Cuba; (iii) Iran; (iv) North Korea; and (v) Syria; and

    d) For Agents that do not have a website and/or are owned by another company, also conduct the same steps (i.e., (b) – (d)) for the Beneficial Owner, or, if necessary, the owner's owner.

3.6 **Step 5 – Approval/Refusal**

No High Risk Agent can be on-boarded without approval of the Compliance Officer. The Compliance Officer and/or the business has the right to escalate any case to the Zone's Compliance Committee for a decision in relation to on-boarding/approval. Rationale for the decision to on-board an Agent must be maintained on file.

Compliance Committee

Ras Al Khaimah ("RAK") Zones' Compliance Committee is a governance body established by the Board of the Investment and Development Office to oversee the implementation of the Compliance Programme at each of the Zones.

The RAK Compliance Committee will review requests escalated by the Zones to reject, approve, or continue to provide services to HRCs in cases where the Zones' Compliance Committee or the Compliance Officer deem it appropriate and necessary.

The Zone shall not enter into a business relationship with an Agent in any of the following categories:

- Where CDD cannot be completed satisfactorily.
- Where the Agent is a listed Sanctions Target.
- Where any of the Agent's Beneficial Owners, directors/senior managers or power of attorney holders are listed Sanctions Targets.
- Where the Agent or any of its Beneficial Owners, directors/senior managers or power of attorney holders is (a) resident, registered or incorporated in an Embargoed Territory; or (b) owned or controlled by, or operating as agents of, the Government of an Embargoed Territory or the Government of Venezuela.
- Where the Zone considers in its absolute discretion that the Agent presents unacceptable reputational risk to the Zone.
- Where the Zone considers in its absolute discretion that the Agent is outside the Zone's risk appetite.
- Where the Agent is or is owned by a bearer share corporation or shell bank.
- Where the Agent (or its Beneficial Owners or directors/senior managers) are: (i) wanted by Interpol; (ii) wanted by international authorities for organized crime-related offenses; and (iii) accused (within the past 7 years) or wanted by international authorities for money-laundering or terrorism-related crimes.

Formal written agreement must be established with each Agent specifying, inter alia, the maximum duration, notice terms (typically 30 days) and remuneration basis. Such agreement must also document applicable sanctions and anti-bribery clauses (*i.e.,* that agent will comply with applicable Anti-bribery legislation).

3.7 **Step 6 – Periodic Reviews/ Renewals/ Audits**

Renewals

Core CDD information should be reviewed and refreshed as part of the Agent renewal process.

This involves checking that all documents remain active/current, including (but not limited to):

- Trade Licence
- Tenancy/Lease Agreements
- Organisation Chart
- AML and Sanctions Compliance Manual

RAKICC:

If the due diligence on Agents to which the Zone outsources any aspect of the CDD process identifies any red flags or concerns relevant to this Policy, the Agent must undergo a compliance audit by a reputable audit firm to confirm that the Agent has implemented a compliance policy in line with the standards in this document, and that the Agent applies CDD procedures no less extensive and effective than those set out in these operating procedures. Such audits can also be requested by the Compliance Officer at their discretion.

In addition, the compliance checks, risk-rating process and, *where applicable*, EDD described at **Steps 1-4** above must be checked and (as necessary) re-completed as part of renewal process.

Other Changes

CDD, the compliance checks, risk-rating and, *where applicable*, EDD must also be repeated/refreshed whenever the Zone suspects that information previously obtained is no longer reliable or adequate. If at any time an Employee becomes aware that the Zone lacks sufficient information or documentation concerning a person's identification or develops a concern about the accuracy of current information or documentation, they must inform the Compliance Officer and the Zone will promptly obtain appropriate material to verify the person's identity.

Agents are instructed to immediately notify the Zone of any changes in their shareholders or directors/managers so that the Zone can update the CDD information. Any change to

directors, managers, shareholders or Beneficial Owners of an entity must be subject to CDD as outlined in section 1.1 above.

3.8 **Data recording and Ongoing Screening**

Information collected as part of the CDD process is recorded in an electronic database (*i.e.,* SAP/Sales Force); as follows:

- Full name of the Agent
- Full name, local (*if any*) and home country address, including country of residence, registration or incorporation, nationality and country of passport(s) held (*if relevant*) of all:

  (a) individuals who are Beneficial Owners;

  (b) directors/senior managers; and

  (c) power of attorney holders.

Information will be entered into Sales Force on a maker/checker (*i.e.,* four-eye) basis to ensure accuracy.

The database also should include a description of the Client's business, including whether the Client has exposure to the Embargoed Territories or other Sanctions Targets.

All of this data should be stored electronically in a format that is easily searchable.

This information shall be subject to regular and ongoing screening (using the screening solution provided by Accuity) on a daily basis against updates to the official sanctions-related lists administered by the UAE, US and the EU (including the UK) to detect the possible addition of a Client or associated persons to a Sanctions list. In addition, when the local and home country address, nationality and country of passport(s) held fields in SAP/Sales Force are updated, these fields should be screened against a set of geographic search terms for the Embargoed Territories.

3.9 **Record Keeping**

Copies of the evidence obtained to satisfy CDD is kept for a period of five years from the date on which the business relationship with the Agent comes to an end (for example, the date of expiration/termination of a lease/licence/registration).

3.10 **AGENT EXIT PROCEDURES**

Where CDD cannot be completed satisfactorily, including in regard to the Beneficial Ownership of the Agent, the Zone will make every reasonable effort to terminate any existing business relationship, will not provide a service to or for the Agent, will not establish a

business relationship or carry out an occasional transaction with the Agent and may consider making a suspicious transaction report.

4. EMPLOYEE AWARENESS AND TRAINING

The Zone conducts an ongoing anti-money laundering, counter terrorist financing and Sanctions training programme, which must be attended by all relevant Employees. Those concerned are advised when the course should be attended and when refresher training is due.

This training covers:

- the identity and responsibilities of the Compliance Officer
- applicable legislation and regulations relating to money laundering and Sanctions and the Zone's internal AML/CTF and Sanctions procedures, policies, systems and control and any changes to these;
- the effect on the Zone, Employees and business partners of breaches of applicable legislation and regulations concerning money laundering and Sanctions;
- money laundering and Sanctions risk, trends and techniques, how to recognise and handle suspicious transactions and the Zone's arrangements regarding the making of an internal suspicious transaction report;
- the use of relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions from relevant authorities; and
- requirements in relation to identification and ongoing due diligence of business relationships and scrutiny of transactions.

The Compliance Officer has overall responsibility for the AML/CTF and Sanctions training programme and is responsible for ensuring that training is up-to-date with money laundering trends and techniques and appropriately tailored to the Zone's different activities, services and business relationships.

Appropriate and frequent refresher training is also given to all relevant Employees. All relevant Employees are required to attend an AML/CTF and Sanctions training session at least once every 12 months. Employees should be aware that all AML/CTF and Sanctions training is mandatory and accurate details of the Zones' AML/CTF training is recorded.

Information and training is provided to all new relevant employees and remains available to all employees. Should any employee wish to access information on the Zone's AML/CTF and Sanctions policies, procedures, systems or controls, they should contact the Compliance Officer, who will provide such information.

Training records (maintained for 5 years) include:

- a copy of the training materials
- details of who provided training, if provided externally
- a list of Employees who have completed training, with dates, and their signatures (confirming their understanding of the obligations) or electronic training records
- an up-to-date training schedule.

5. AUDIT

The AML and Sanctions policies and these procedures shall be reviewed once every two years, (frequency can be increased to annual in response to significant compliance findings) by an independent audit or compliance function to ensure that they are effective and in line with legal requirements and industry best practices and, if necessary, the policy and procedures shall be updated.

The Zone's AML/CTF and Sanctions systems and controls will also be reviewed by an independent audit or compliance function least once every two years including sample testing. They will check adherence to the policies, controls and procedures and review how effective these are, recommending and implementing improvements following such reviews (for example to reflect changes in the business environment).

* * *

APPENDIX 1 – US PERSON INSULATION

"**US Persons**" include: anyone while physically present in the United States; any US citizen or green card holder, wherever located (including dual nationals of the US and another country); any US-incorporated entity, or anyone employed by a US entity. Non-US entities that are US-owned or controlled are also subject to compliance obligations under US Cuba and Iran sanctions.

In the absence of an applicable license or exception, US economic sanctions prohibit the involvement of US Persons in transactions with "**US Sanctions Targets**," including:

- Persons, entities and vessels listed by the US Department of Treasury's Office of Foreign Assets Control ("**OFAC**") and companies owned 50% or more by them;
- The Embargoed Territories and their governments (*presently,* Cuba, Iran, North Korea, Syria and Crimea), as well as the Government of Venezuela, companies owned or controlled by such governments or persons acting as agents for them; and
- All activity with, in or through the Embargoed Territories.

Accordingly, all employees who are US Persons, (including non-US citizens while in the United States) must not participate in or otherwise support or facilitate transactions involving US Sanctions Targets unless Compliance confirms[6] that OFAC has licensed or otherwise permitted such transactions.[7]

Specifically, if you are a US Person, including a non-US citizen while located in the United States:

1. Do not provide any commercial advice, assistance or other support in connection with business involving a US Sanctions Target (unless permitted to do so under OFAC sanctions);
2. Do not supervise, authorize or approve any business involving a US Sanctions Target or manage or direct the conduct of other employees in regard to such business (unless permitted to do so under OFAC sanctions);
3. Do not participate in the re-design or restructuring of any transactions, operations, products or services for the purpose of facilitating business involving a US Sanctions Target (unless permitted to do so under OFAC sanctions);

[6] Compliance approval is required for all transactions that involve a US Sanctions Targets.

[7] The SSI List ("sectoral") Sanctions (involving Russia) and US Sanctions against the Government of Venezuela do not prohibit US Person involvement in all transactions with SSI Listed or Government of Venezuela companies. Consult the Compliance Officer if you have questions about the transactions to which this insulation policy applies.

4. Do not provide corporate services (*e.g.*, accounting, logistics, contract administration, technical services) specifically to support business involving a US Sanctions Target (unless permitted to do so under OFAC sanctions).

5. Do not refer business involving a US Sanctions Target to any other person or issue any powers of attorney in relation to specific transactions with a US Sanctions Target (unless permitted to do so under OFAC sanctions).

6. Do not provide any services listed above in connection with an extension of debt of longer than 14/60/30 days' maturity or new equity, as applicable, of SSI Sanctions Targets (Directives 1-3).

Employees who are not US Persons must not involve US Persons, exports of US-origin goods or services, or the US financial system in any business involving a US Sanctions Target (unless permitted to do so under OFAC sanctions).

Thus, if you are not a US Person and your transaction involves a US Sanctions Target without benefiting from an OFAC license or other OFAC authorization:

1. Do not work on that transaction while you are in the United States;

2. Do not ask a US Person (including a US citizen or green card holder outside the United States) to assist you with that transaction;

3. Do not discuss that transaction with a US Person, except to alert them to the need for compliance with this protocol or raise an OFAC compliance issue;

4. Do not include US Persons in e-mail chains in furtherance of that transaction;

5. Do not attempt to involve US Persons in that transaction by withholding information about its connection to a US Sanctions Target; and

6. Do not use credit or other assets provided by US Persons to finance transactions with US Sanctions Targets or provide US Persons (*e.g.,* banks) with funds derived from such transaction.

Examples:

The following are examples of actions that would violate this protocol:

- A US citizen employed by the Zone negotiates a lease with a potential client located in Iran or owned by the Government of Iran;

- A non-US employee negotiates the same lease while temporarily working from an office in New York; and

- A US green card holder employed by the Zone in Ras Al Khaimah reviews and approves a license application from a prospective client in Syria.

Insulation of US Person Executive Officers and Board/Committee Members

As noted above, anyone who is a US Person must not approve, authorize, advise on or otherwise provide support or assistance in connection with business involving US Sanctions Targets unless US law permits their involvement in a particular case (*i.e.*, because OFAC has licensed the transaction).

A strict insulation policy therefore applies to any US Persons who may now or in the future serve as a board member, director, officer or committee member of any of the Zones, meaning that they may not participate in any portion of meetings in furtherance of OFAC-restricted business involving a US Sanctions Target.[8]

US Persons therefore should leave the meeting room and/or drop off video/audio conferences during such interval that action is taken specifically in furtherance of OFAC-restricted business with a US Sanctions Target.

> Clarification regarding Compliance Advice: The Zones may seek and consider advice provided by US Persons on compliance with OFAC and other sanctions regulations and the Zones' exposure to sanctions risks. In this context, US Person members of or advisors to the Zones boards and committees may address sanctions compliance issues on behalf of the Zones, while at the same time removing themselves from any commercial planning or decisions in furtherance of OFAC-restricted business with US Sanctions Targets.

Board and committee members, directors and officers who are not US Persons should not include US Persons in emails or other communications regarding the commercial aspects of OFAC-restricted business with US Sanctions Targets (in contrast to requests for compliance advice) and should avoid any other actions that might contradict the insulation policy applicable to US Persons.

* * *

[8] The mere fact that a US Person may know about or become aware of business with a US Sanctions Target, or questions the risks presented by such business, does not violate this protocol, as long as the US Person does not use that information to facilitate such business.

APPENDIX 2 – EU PERSON RECUSAL

"**EU Persons**" include anyone while physically in the territory of the European Union; any national of an EU Member State, wherever located; any EU-incorporated entity, or, for the purposes of this policy, anyone employed by an EU-incorporated entity.

In the absence of an applicable license or exception, EU economic sanctions prohibit the involvement of EU Persons in transactions (directly or indirectly) with any natural or legal persons, entities or bodies included on a list of persons designated by the EU as subject to EU Sanctions ("EU Sanctions Targets") or otherwise in transactions that are prohibited by EU sanctions.

Accordingly, all personnel who are located in the EU, or who are nationals of an EU Member State and located anywhere in our organization must not participate in or otherwise support or facilitate transactions with EU Sanctions Targets or transactions that are otherwise prohibited for EU Persons.

Specifically, if you are an EU Person:

- Do not provide any commercial advice, assistance, approval or other support in connection with business involving an EU Sanctions Target or any transaction that is otherwise prohibited by EU sanctions;

- Do not supervise or authorize any business involving an EU Sanctions Target or any business that is otherwise prohibited by EU sanctions or manage or direct the conduct of other personnel in regard to such business;

- Do not participate in the re-design or restructuring of any transactions, operations, products or services for the purpose of facilitating business involving an EU Sanctions Target or business that is otherwise prohibited by EU sanctions;

- Do not provide corporate services (*e.g.*, accounting, logistics, contract administration, technical services) specifically to support business involving an EU Sanctions Target or business that is otherwise prohibited by EU sanctions.

* * *

APPENDIX 3 – CLIENT CDD CHECKLIST

Name/proposed name of entity/establishment		
Was the Entity type captured?	☐ Yes ☐ No	
Was the Entity's registered address captured?	☐ Yes ☐ No	
Was the principal place of business[9] **captured?**	☐ Yes ☐ No	
Was the proposed license type captured?	☐ Yes ☐ No	
Were the actual/ proposed business activities of the entity identified? ***A generic business activity description (such as "management services" or "general" trading) is not sufficient.***	☐ Yes ☐ No	
Does/will the entity engage in any of the following High Risk Businesses (high risk trigger)? If so, please consult Compliance to conduct Enhanced Due Diligence	☐ Activities in defence industry	☐ Energy
	☐ Aviation services	☐ High value/luxury good dealers
	☐ Charities or non-profit organizations	☐ Insurance activities (not including brokers and agents)
	☐ Coins investment and trading	☐ Lending activities
	☐ Dealers in precious metals and stones	☐ Money Services Businesses (MSB)
	☐ Dealing in bitcoin and other cryptocurrencies	☐ Mining
	☐ Debt collection agencies	☐ Trusts
Have you captured full name, local (if any) and home country address, date of birth, and nationality(-ies) (including all nationalities held) of <u>ALL proposed</u>	☐ Yes ☐ No	

[9] An entity's principal place of business includes the country of the entity's main operating office.

directors/ senior managers, as well as, in each case, evidence of identity?	
Have you obtained all the required information for directors which are corporate entities?	☐ Yes ☐ No
Have you captured full name, local (if any) and home country address, date of birth, and nationality(-ies) (including all nationalities held) of ALL Beneficial Owners, as well as in each case, evidence of identity?	☐ Yes ☐ No
Have you captured full name, local (if any) and home country address, date of birth, and nationality(-ies) (including all nationalities held) of any individual acting on behalf of the entity pursuant to a Power of Attorney or by other means, as well as evidence of identity?	☐ Yes ☐ No ☐ N/A
Have you obtained a valid copy of the Power of Attorney, legally attested by a relevant authority?	☐ Yes ☐ No ☐ N/A
Have you received a filled sanctions policy questionnaire?	☐ Yes ☐ No
Has the Client answered "Yes" to any questions within the Sanctions Policy Questionnaire? If so, please consult Compliance to conduct Enhanced Due Diligence	☐ Yes ☐ No
Have you reviewed the Entity's registered address as well as home country address information, issuing country of passport(s) held and nationality of the Entity's Beneficial Owners, directors/senior managers and power of attorney holders for reference to a Sanctioned Country?	☐ Yes ☐ No
Did this review show any reference to a Sanctioned Country? If so, please consult Compliance to conduct Enhanced Due Diligence	☐ Yes ☐ No
Are there any directors, senior managers, Beneficial Owners, power of attorney holders who are resident, registered or incorporated in a high risk country? (see Appendix 4) If so, please consult Compliance to conduct Enhanced Due Diligence	☐ Yes ☐ No
Having referred to the Red Flag Guidance at Appendix 5, are there any other present factors which indicate increased risk? If so, please consult Compliance to conduct Enhanced Due Diligence	☐ Yes ☐ No

Please confirm standard due diligence has been completed.	☐ Yes ☐ No
What risk rating has been given to the Entity?	☐ Standard Risk ☐ High Risk
Provide details of why this risk rating has been given to the Entity	
Name of the person preparing the CDD form	
Date	
For High Risk entities only: **Has Compliance approval of the on-boarding or renewal of the Entity been provided?**	☐ Yes ☐ No
Date of Approval	
Name of the Compliance Officer providing approval	

APPENDIX 4 – HIGH RISK COUNTRIES MATRIX

This Policy takes the approach of adopting the European Commission list of third countries with strategic deficiencies in their anti-money laundering and counter-terrorist financing frameworks.

As of 2nd of April 2019, the jurisdictions are:

- Afghanistan
- Bosnia and Herzegovina
- Democratic People's Republic of Korea
- Ethiopia
- Guyana
- Iran
- Iraq
- Lao PDR
- Pakistan
- Sri Lanka
- Syria
- Trinidad and Tobago
- Tunisia
- Uganda
- Vanuatu
- Yemen

In addition, due to a tightening sanctions regime against **Venezuela**, and regional sanctions in place against **Qatar** in the GCC, it is deemed appropriate to add both Venezuela and Qatar to the list of High Risk Countries.

HIGH RISK COUNTRIES

Afghanistan, Bosnia and Herzegovina, Democratic People's Republic of Korea*, Ethiopia, Guyana, Iran*, Iraq, Lao PDR, Pakistan, Qatar, Sri Lanka, Syria*, Trinidad and Tobago, Tunisia, Uganda, Vanuatu, Venezuela, Yemen.

*Also Embargoes Territories

* * *

APPENDIX 5 – RED FLAG GUIDANCE

The Zone provides the basis for legitimate economic activities in RAK. Companies in the Zone have many genuine uses such as business, finance, family settlements, estate and corporate planning.

However, there is a risk that the Zone may be misused by criminals for illegal purposes such as hiding the Beneficial Ownership of assets, use of virtual offices, mail forwarding or serviced offices to add a layer of anonymity, legitimating the integration of the proceeds of crime or layering of crime proceeds through various forms of investment such as in the stock market.

The Zone does not routinely deal directly with a Client's funds, but will be able to focus on the persons it is transacting with and the nature of the services provided. In view of the risks involved, the Zone must be vigilant at all times and report any suspicious activity where necessary.

The following are some examples of risk indicators in relation to the services provided:

Risk Factors may include:

- establishment of multi-jurisdictional and/or complex structure of corporate entities and or trusts without obvious commercial rationale
- the use of multiple companies or trusts which adds a layer of complexity to ownership, particularly where those layers seem unnecessary, for example, trusts owning trusts or offshore shell companies
- professionals assisting Clients to use schemes that can disguise income, assets and ownership
- Clients or professionals being evasive or reluctant to provide required CDD information or documentation or where ownership is said to be confidential
- the number of intermediaries or professionals used seems excessive or there seems to be no need for a professional
- excessive or unnecessary use of nominees
- intermediary chains where trust or company service providers act as nominee director for large numbers of limited companies
- intermediary chains where trust or company service providers market themselves and their

jurisdictions as facilitating anonymity and disguised asset ownership

- payments (local or foreign) are made or received in cash, or without a clear connection to the actual activities of the corporate entity
- use of off-shore bank accounts without legitimate economic requirement and where sources and/or destinations of funds are unknown
- establishing a company primarily for the purpose of collecting funds from various sources which are then transferred to local or foreign bank accounts that have no apparent ties with the company
- large movement of funds through a company with no good legal or commercial reason or an absence of any underlying transactions
- the transfer of funds in the form of "loans" to individuals from trusts and non-bank shell companies facilitating a system of regular transfers to these corporate vehicles from the “borrowing” individuals in the form of “loan repayments”
- incorporation of a company by a non-resident with no links or activities in the UAE or the jurisdiction where the company is established
- the money flow generated by a company is not in line with its underlying business activities
- shares owned by companies and trusts in off-shore jurisdictions or high risk third countries or countries with high levels of corruption, illicit drug dealing or organised crime
- multiple appearances of the same parties in transactions over a short period of time
- Client unwilling or refuses to provide information including documentary proof of himself/herself or Beneficial Owner(s) of trusts or companies
- Client appears to carry out transactions for themselves or on behalf of the company that does not correspond with their background
- the Beneficial Ownership is veiled in complexity making it impossible to determine
- client is secretive about the reasons for and way a company structure is being set up
- client favours legal entities that are not transparent or do not require registration of Beneficial Ownership information
- client wants to use jurisdictions with, for example, weak anti money laundering laws or controls, limited corporate registration requirements, where there is no requirement to update ownership changes, unrestricted bearer share usage, secrecy laws or limited Beneficial Ownership information requirements

- searches on a Client or associate show, for example, adverse media attention, disqualification as a director, convictions for dishonesty or association with bribery in relation to contract procurement

- the Client is, or appears to be, acting on behalf of another person, an unwillingness to give the names of the persons they represent

- the person acting as a director or representative does not appear to be a suitable representative or does not appear to have the expertise that the role requires clients whose owners or directors have a lavish lifestyle that appears to exceed known sources of income

- frequent changes in ownership, officers, beneficiaries or trustees.

* * *

APPENDIX 6 AGENT CDD CHECKLIST

RAKEZ

Full name of Agent	
Have you received a letter of application to be an approved Agent?	☐ Yes ☐ No
Was the registration number captured?	☐ Yes ☐ No
Was the Agent's registered address captured?	☐ Yes ☐ No
Was the principal place of business [10] captured?	☐ Yes ☐ No
Have you captured full name, local (if any) and home country address, date of birth, and nationality(-ies) (including all nationalities held) of <u>ALL directors/ senior managers</u> of the Agent, as well as, in each case, evidence of identity?	☐ Yes ☐ No
Have you captured full name, local (if any) and home country address, date of birth, and nationality(-ies) (including all nationalities held) of <u>ALL Beneficial Owners</u> of the Agent, as well as, in each case, evidence of identity?	☐ Yes ☐ No
Have you received the Agent's Business Plan?	☐ Yes ☐ No
Have you received a copy of the Agent's Professional Licence in the UAE & Tenancy/Lease contract for UAE office?	☐ Yes ☐ No
Have you received a copy of the Agent's AML, CTF and Sanctions policies and procedures?	☐ Yes ☐ No
Have you received an undertaking that AML, CTF and Sanctions Policies and Procedures are commensurate with the RAKEZ Compliance Policy?	☐ Yes ☐ No
Have you received the Agent's acknowledgement of receipt and understanding of the RAKEZ Compliance Policy?	☐ Yes ☐ No

[10] An entity's principal place of business includes the country of the entity's main operating office.

Have you received the Non-Disclosure Agreement?	☐ Yes ☐ No
Have you received the Sanctions Policy Questionnaire?	☐ Yes ☐ No
Has the Client answered "Yes" to any questions within the Sanctions Policy Questionnaire? If so, have you referred to the Compliance team? If so, please consult Compliance to conduct Enhanced Due Diligence	☐ **Yes** ☐ **No**
Have you reviewed the Agent's registered address as well as home country address information, issuing country of passport(s) held and nationality of the Agent's Beneficial Owners, directors/senior managers and power of attorney holders for reference to a Sanctioned Country?	☐ **Yes** ☐ **No**
Did this review show any reference to a Sanctioned Country? If so, please consult Compliance to conduct Enhanced Due Diligence	☐ Yes ☐ No
Are there any directors, senior managers, Beneficial Owners, power of attorney holders who are resident, registered or incorporated in a high risk country? (see Appendix 4)? If so, please consult Compliance to conduct Enhanced Due Diligence	☐ Yes ☐ No
Having referred to the Red Flag Guidance at Appendix 5, are there any other present factors which indicate increased risk? If so, please consult Compliance to conduct Enhanced Due Diligence	☐ Yes ☐ No
Please confirm standard due diligence has been completed.	☐ Yes ☐ No
What risk rating has been given to the Agent?	☐ Standard Risk ☐ High Risk
Provide details of why this risk rating has been given to the Agent.	
Name of the person preparing the CDD form	
Date	
For High Risk entities only: **Has Compliance approval of the on-boarding of the Agent been provided?**	☐ Yes ☐ No

Date of Approval	
Name of Compliance Officer providing approval	

RAK ICC

Full name of Agent	
Have you received a letter of application to be an approved Agent?	☐ Yes ☐ No
Was the registration number captured?	☐ Yes ☐ No
Was the Agent's registered address captured?	☐ Yes ☐ No
Was the principal place of business [11] captured?	☐ Yes ☐ No
Have you captured full name, local (if any) and home country address, date of birth, and nationality(-ies) (including all nationalities held) of <u>ALL directors/ senior managers</u> of the Agent, as well as, in each case, evidence of identity and CV of each director?	☐ Yes ☐ No
Have you captured full name, local (if any) and home country address, date of birth, and nationality(-ies) (including all nationalities held) of <u>ALL Beneficial Owners</u> of the Agent, as well as, in each case, evidence of identity?	☐ Yes ☐ No
Have you obtained all the required information for shareholders which are corporate entities?	☐ Yes ☐ No
Have you received the Agent's HR organisational chart?	☐ Yes ☐ No
Have you received the Agent's Business Plan?	☐ Yes ☐ No
Have you received a copy of the Agent's Professional Licence in the UAE & Tenancy/Lease contract for UAE office?	☐ Yes ☐ No
Have you received a copy of the Agent's AML, CTF and Sanctions policies and procedures?	☐ Yes ☐ No
Have you received an undertaking that AML, CTF and Sanctions Policies and Procedures are commensurate with the RAKEZ Compliance Policy?	☐ Yes ☐ No

[11] An entity's principal place of business includes the country of the entity's main operating office.

Have you received the Agent's acknowledgement of receipt and understanding of the RAKEZ Compliance Policy?	☐ Yes ☐ No
Have you received the Non-Disclosure Agreement?	☐ Yes ☐ No
Have you received the Sanctions Policy Questionnaire?	☐ Yes ☐ No
Has the Client answered "Yes" to any questions within the Sanctions Policy Questionnaire? If so, please consult Compliance to conduct Enhanced Due Diligence	☐ **Yes** ☐ **No**
Have you reviewed the Agent's registered address as well as home country address information, issuing country of passport(s) held and nationality of the Agent's Beneficial Owners, directors/senior managers and power of attorney holders for reference to a Sanctioned Country?	☐ **Yes** ☐ **No**
Did this review show any reference to a Sanctioned Country? If so, please consult Compliance to conduct Enhanced Due Diligence	☐ Yes ☐ No
Have you received name and details of the Agent's compliance officers, including CV?	☐ Yes ☐ No
Are there any directors, senior managers, Beneficial Owners, power of attorney holders who are resident, registered or incorporated in a high risk country? (see Appendix 4)? If so, please consult Compliance to conduct Enhanced Due Diligence	☐ Yes ☐ No
Having referred to the Red Flag Guidance at Appendix 5, are there any other present factors which indicate increased risk? If so, please consult Compliance to conduct Enhanced Due Diligence	☐ Yes ☐ No
Please confirm standard due diligence has been completed.	☐ Yes ☐ No
What risk rating has been given to the Agent?	☐ Standard Risk ☐ High Risk
Provide details of why this risk rating has been given to the Agent.	
Name of the person preparing the CDD form	

Date	
For High Risk entities only: **Has Compliance approval of the on-boarding of the Agent been provided?**	☐ Yes ☐ No
Date of Approval	
Name of Compliance Officer providing approval	

APPENDIX 7 – SANCTIONS POLICY QUESTIONNAIRE

ZONE NAME – Sanctions Policy Questionnaire

It is the policy of the Zone to fully comply with all sanctions laws and regulations of the United Arab Emirates, United Nations, United States and European Union (including the United Kingdom), as well as other such laws and regulations, when applicable to its business (collectively, "**Sanctions**").

Legal entity name: XXX	
Exposure to sanctioned countries and targeted sanctions regimes	
To the best of your knowledge, is the company or any of the company's Related Parties[12] a "**Sanctions Target,**" which includes persons or entities that are: • Listed by the United Arab Emirates, United Nations, United States, European Union or the United Kingdom as a target of Sanctions; • Owned or controlled by, or operating as agents of, the Governments of Cuba, Iran, North Korea, Syria or Venezuela; or • Resident or domiciled in Iran, Syria, North Korea, Cuba or Crimea (collectively, the "**Embargoed Countries**")**?** *If you have answered "Yes", please provide further details*	Yes ☐ No ☐
To the best of your knowledge, is the company or any of the company's Related Parties owned by a Sanctions Target? *If you have answered "Yes" please provide further details, including a description of the ownership interest (e.g., % of shares held) held by the Sanctions Target*	Yes ☐ No ☐
To the best of your knowledge, does the company or company's Related Parties have any presence in (*i.e.,* registered office, branch office, subsidiary or other operations, address, principal place of business), or "**Business Activity**" (*i.e.,* sales or purchases, including through agents or intermediaries, investments, transhipments, etc.) with or involving, directly or indirectly, and Embargoed Country?	Yes ☐ No ☐

[12] Related Parties include but are not limited to shareholders, beneficial owners, key controllers (*e.g.*, directors and senior managers), trustees, founders/grantors/settlors and beneficiaries.

If you have answered "Yes", please provide further details, including the % of business involving an Embargoed Country	
To the best of your knowledge, does the company have any Business Activity with or involving, directly or indirectly, a Sanctions Target? *If you have answered "Yes", please provide further details, including the % of business involving a Sanctions Target*	Yes ☐ No ☐

We confirm that all of our business with, through or involving [insert name of the Zone] will not involve a sanctioned country (at present, Crimea, Cuba, Iran North Korea or Syria), including goods procured from or transhipped through a sanctioned country, or violate or cause [insert name of the Zone] to violate any economic or financial sanctions or trade embargoes implemented, administered or enforced by the United Arab Emirates, the United Nations, United States, European Union, United Kingdom or other relevant sanctions authorities."

Date:

Authorised signatory of the client: