UNITED GULF BANK B.S.C. (c)

ANTI-MONEY LAUNDERING & COMBATING OF FINANCIAL CRIME POLICY AND PROCEDURES MANUAL

Date of Last Review: February 2025	Date of Current Review: February 2026

Contents

Glossary

AML	Anti-Money Laundering
BB	Burgan Bank K.P.S.C. – the parent of UGB
Board	Board of Directors of UGB
CBB	Central Bank of Bahrain
CDD	Customer Due Diligence
CFT	Combating Terrorist Financing
DMLRO	Deputy Money Laundering Reporting Officer
EDD	Enhanced Due Diligence
FATF	The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. As of 2022 the FATF had 39 full members, comprising 37 member jurisdictions and two regional organizations. (European Commission; Gulf Cooperation Council). The FATF also works in close co-operation with a number of international and regional bodies involved in combating money laundering and terrorism financing.
FID	Financial Intelligence Directorate, General Directorate of Anti-Corruption and Economic and Electronic Security, Ministry of Interior
GAFC	Group Anti Financial Crime Department of Burgan Bank K.P.S.C. – the parent of UGB.
IIS	Institutional Information System: access to this is available with the Compliance & MLRO.
KYC	Know Your Customer
MLRO	Money Laundering Reporting Officer
NCCT	Non-Cooperative Countries or Territories as defined by the FATF.
OPERATIONS	The Operations Department of UGB
PEP	Politically Exposed Person.
PF/WMD	Proliferation Financing refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological

	weapons of mass destruction (WMD) and their means of delivery. The risk to an institution stems from the potential breach, non-implementation or evasion of targeted financial sanctions imposed as a result of the above.
RBA	Risk based assessment – the process to identify, assess, monitor, manage and mitigate ML/TF/PF risks to which the Bank is exposed through transactions conducted by its customers. The risk assessment must enable the Bank to understand how, and to what extent, it is vulnerable to ML/TF/PF.
Securities	Securities means shares or bonds issued by shareholding companies, government debt instruments and the following financial instruments: a. Shares in companies and other Securities equivalent to shares in companies or other entities, and depositary receipts in respect of shares. b. Bonds or other forms of debt, including depositary receipts in respect of such Securities ; c. Warrants, Units, rights or interests (however described) of the participants in a collective investment scheme; d. Options, futures and any other derivative contracts relating to commodities that must be settled in cash, or may be settled in cash at the option of one of the parties (otherwise than by reason of a default or other termination event); e. Options, futures and any other derivative contract relating to commodities that can be physically settled; f. Units to Real Estate Investment Trusts (REIT). g. Index tracking products including Islamic indices. h. Any other financial instrument approved as a financial instrument by the CBB for the purpose of trading such instrument on an exchange; and j. Islamic Securities, being those financial instruments that are Shari'a compliant.
UGB	United Gulf Bank B.S.C. (c), also referred to as the Bank
UGH	United Gulf Holding Company B.S.C. (UGH, the Company) – this is an entity with which UGB has a service level agreement to provide AML services.

1. Introduction

1.1 Purpose

The Central Bank of Bahrain (CBB) requires all banks to establish comprehensive policy and procedures (PPM) that documents the measures undertaken by financial institutions to combat and limit their vulnerability to anti-money laundering, breach of sanctions, terrorism financing and counter proliferation financing efforts.[1] This PPM describes the tools, methodology, and systems that assist United Gulf Bank B.S.C. (c) (UGB, the Bank) to implement customer due diligence, ongoing transaction monitoring, reporting obligations and the application of a risk based approach.[2]

The Manual is aimed at assisting members of UGB's Board of Directors, Senior Management and staff to discharge their responsibilities related to customer due diligence, electronic transfers, reporting and the functions of the Money Laundering Reporting Officer.

Employees in particular must know:

- How to recognize money laundering and the action they will take if they do come across any such act.
- Be aware of the Bank's Policy and follow the Bank's procedures on AML.
- Be alert for anything suspicious when handling financial transactions.
- Report suspicious transactions internally to the MLRO in line with internal procedures.
- Be aware of their personal legal obligations and the legal obligations of the Bank, in relation to implementing AML procedures.
- The different penalties for non-compliance

It is the responsibility of the Board of Directors, Senior Management, MLRO, Deputy MLRO and all staff of the Bank to adhere to AML standards and ensure that there are appropriate systems and controls for compliance with the requirements of the CBB and the Bahrain Bourse's to limit vulnerability to financial crime[3].

1.2 Scope of the PPM

This PPM covers the operations of UGB and United Gulf Holding Company B.S.C. (UGH, the Company) with whom the Bank has signed a service level agreement that includes providing AML compliance services. It should be recognized that there is no separate PPM for UGH, as the company is not permitted to undertake transactions for its customers under the terms of its license. UGH's AML activities mainly relate to the due diligence of the Company's regulated financial counterparties. UGH's risk assessment will hence be basic and is based on the simplified due diligence permitted by the CBB.

1.2.1 Responsibilities of UGB as the parent

1 FC-A.1.2, Volume 1, CBB Rulebook.
2 FC-1.1.2G
3 FC-4.1.5

It is the responsibility of UGB as the head of a financial group, to ensure that each of its financial subsidiary/ies implement groupwide programs against AML and terrorist financing.[4] While each subsidiary is committed to having a robust AML framework policies, and procedures, it should be recognized that the extent of AML compliance is subject to the requirements of the regulators of the jurisdictions in which the subsidiaries operate. All subsidiaries have been informed by UGB's MLRO of the need to implement groupwide programs against money laundering and terrorist financing, including policies and procedures for sharing information within the group for AML/CFT purposes.

In order to seek assurance from UGB's subsidiaries, a questionnaire covering the above matters will be circulated by UGB at the end of each year. Each of the MLRO's of the Bank's financial subsidiaries has to affirm through responses to UGB's MLRO, that there are adequate controls. A copy of this is included in Appendix 2 – Annual AML Questionnaire from UGB's financial subsidiaries. UGB's and UGH's subsidiaries have also been asked to keep UGB's MLRO of any AML issues that have been notified to or queried by their local regulators.

Reference is made in this PPM to the tenets of the Personal Data Protection Law No. 30 of 2018 wherein the personal, sensitive data of customers must be stored, safeguarded and used only for legitimate purposes as defined by the law. Access to personal data is restricted to the MLRO, Deputy MLRO, and staff in the Compliance, Internal Audit and Operations Departments.

1.2.2 Responsibilities of UGB's subsidiaries

The subsidiaries' AML policy must cover their branches/downstream subsidiaries and include:

- The development of internal policies, procedures, and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees.

- An ongoing employee training program.

- An independent audit function is to test the system.

- Policies and procedures for sharing information required for the purposes of CDD and money laundering and terrorist financing risk management. This includes incorporating risk management procedures with respect to the conditions under which a customer may utilize the business relationship.[5]

- The provision at group-level compliance, audit, and/or AML/CFT functions of customer, account and transaction information from branches and subsidiaries when necessary for AML/CFT purposes; and

4 FC-B.2.1

5 FC-B.2.4

- Adequate safeguards on confidentiality and use of information exchanged

- Subsidiaries also have to be cognizant of the CBB's rules on financial crime, as the CBB requires UGB **and** its subsidiaries operating in the Kingdom of Bahrain and in foreign jurisdictions, to follow the rules of Module FC. This documents the standards set by regulatory authorities in Bahrain with respect to AML/ CFT/ PF procedures, systems and controls.[6] Should there be a situation where the subsidiaries' jurisdiction prevents the implementation of the robust AML standards, the respective MLRO must notify UGB's MLRO who will in turn immediately inform the CBB in writing[7].

- It is also the responsibility of UGB's financial subsidiary/ies to provide the Bank's MLRO with an agreed upon procedures report from their external auditors/ external consultants, that documents the adherence of their AML program with the tenets of Module FC. This has to be provided by 15 June every year. The MLRO in turn will submit this to the CBB within the stipulated deadline of 30 June. If the services of an external consultant are used, UGB and its subsidiaries have to ensure that the personnel conducting the review are qualified, skilled and have adequate experience to conduct such a review. At least two people will be asked to work on the report (one of whom is a team leader). The MLRO will ascertain that they have:
  - A minimum of 5 years' professional experience dealing with the AML/CFT issues
  - Formal AML/CFT training.[8]

1.2.3 Responsibilities of UGB to its parent – Burgan Bank K.P.S.C.

UGB is classified as a subsidiary of Burgan Bank K.P.S.C. Under the rules of Kuwait, the Bank has the responsibility of

- Ensuring that applicable AML requirements are complied with through the implementation of an adequate policy, procedures, systems, processes and controls;

- Ensuring that the parents AML standards, as communicated and amended from time to time, are implemented within agreed timelines;

- Assessing the AML compliance status of its subsidiaries / affiliates, and reporting any AML compliance, business and / or reputation risks and issues to Burgan Bank's Group Anti Financial Crime unit (GAFC)

- Seeking advice from GAFC on matters that may require clarification and information; and

- Submitting regular reports as required by their GAFC within agreed timelines.

6 FC-B.2.1

7 FC-B.2.2

8 FC-4.3.2C

1.3 Frequency of Review

This PPM will be documented and reviewed **annually** by UGB's Board of Directors.[9] The documentation and the Board's review and approval will be made available upon request to the external auditors of the Bank, regulators, and financial counterparties with whom UGB has a correspondent or Treasury relationship. Recognizing the importance of enforcing AML standards, the Board authorizes UGB's CEO, MLRO, Deputy MLRO and members of the Management Committee to seek and share information for combating AML/CFT/PF withBurgan Bank and the KIPCO Group.[10]

9 FC-2.1.1
10 FC-B.2.4

2. Definition of Money Laundering

The Financial Crime Module of the CBB Rulebook – Volume1 and the AML Law of the Kingdom of Bahrain (Decree Law No. 4 of 2001), require Banks and other institutions to put in place procedures to prevent criminals from using the financial 'system' to launder "tainted" money.

2.1 What is money laundering?

Money laundering is not just the attempt to disguise money derived from illegal activities. It includes any transaction or series of transactions that seeks to conceal or disguise the nature or source of proceeds derived from illegal activities, including drug trafficking, terrorism, organized crime, fraud, tax evasion, terrorism, and other crimes.

Generally, the money laundering process involves three stages:

- **Placement** - Physically disposing of cash derived from illegal activity. One way to accomplish this is by placing criminal proceeds into traditional financial institutions or non-traditional financial institutions, through_currency exchanges, cryptocurrency exchanges, casinos, or check-cashing services.

- **Layering** - Separating the proceeds of criminal activity from their source using layers of financial transactions. These layers are designed to hamper the audit trail, disguise the origin of funds, and provide anonymity. Some examples are the early surrender of an annuity without regard to penalties, fraudulent letter of credit transactions, the illicit use of bearer shares to create layers of anonymity for the ultimate beneficial owner of the assets, holding assets in an unrelated third party's name or using shell companies as intermediaries in the movement of funds.

- **Integration -** Placing the laundered proceeds back into the economy in such a way that they re-enter the financial system as apparently legitimate funds. Examples of this include depositing the money derived from the sale of assets, real estate etc. into bank accounts.

A financial institution may be used at any point in the money laundering process.

There are personal obligations to every member of UGB's management and staff. Penalties can be incurred for the following:

Transactions	It is an offence to conduct transactions with the proceeds of crime where staff know, or have reason to believe, that funds are the proceeds of criminal activity. This includes receiving, possessing, or concealing the proceeds of such activities.[11]

11 Article 2.1 of the Bahrain Anti Money Laundering Law , 2001

Assistance	Misappropriation of evidence and provision of facilities to persons committing the offence of money laundering are considered to be acts of participation in the offence. The participation offence cannot arise if staff do not know, or have no reason to know, the intent of the person committing the offence.
Destruction	Destruction, misappropriation, concealment or forgery or any document which could be used as evidence in the offence or against the accused. All documents should be preserved for future investigations.[12]
Reporting	It is an offence not to disclose information relating to money laundering to the MLRO or the FID and the CBB. Failure to disclose information regarding money laundering to the FID and the CBB or not co-operating with the FID and the CBB are offences related to money laundering.
Tipping off	It is an offence for anyone to disclose information that might prejudice an investigation by the FID and the CBB.[13] Officers and employees are prohibited from warning or informing (tip off) their customers, the beneficial owner, or other parties of the STR, when information relating to them or their activities is being reported to the relevant authorities.[14]
Responsibility	Where an offence of money laundering is committed by a corporate body, every official of the Bank at the time of the offence is deemed to be guilty of that offence where it is committed deliberately or by gross negligence.

The Bank itself has similar obligations. The decree imposes certain requirements on all financial institutions. These include:

- Account opening procedures - Customer due diligence conducted on a risk based approach.
- Retention of records.
- Recognition and reporting suspicions of money laundering
- Reporting suspicious transactions to regulatory authorities

2.2 What does this mean in practice?

Employees <u>are not</u> committing an offence if they do not know or have no reason to know that the funds relate to the proceeds of criminal activity.

12 Article 2.2 of the Bahrain Anti Money Laundering Law , 2001

13 FC 9.1.1

14 FC-5.2.6

Employees are committing an offence if, knowing or suspecting that someone is involved in criminal activity, and if they:

- assist the suspects to obtain control or retain their proceeds, or
- give them any help in investing or transferring those proceeds,
- advise them that you, or another colleague at the Bank, are suspicious of their activities.

Staff are required to report suspicious transactions to the Money Laundering Reporting Officer (MLRO). If they do not report their suspicion concerning any criminal money, they may need to defend any reprisals and consequences for deliberately assisting the criminal, and that carries a maximum penalty of imprisonment, or a fine, or both. Further details are provided in Section 14. Internal reporting of this PPM.

The MLRO will receive and assess all reports and if warranted, file the STR with Bahrain's Financial Intelligence Directorate and the CBB.

The Bank normally has a duty to refrain from disclosing information to third parties about its customer's account behavior. Exceptions to this are instances when it suspects that the customer may be laundering the proceeds of crime, or if the CBB or the judicial courts of Bahrain require officials to submit documentation on a customer/s account.

3. The Bank's Policy

It is the policy of the Bank that:

- Bahrain's statutory and regulatory obligations to prevent money laundering are fully complied with.
- Proactive management action will be exercised to minimise the risk of the Bank's services being abused for the purposes of laundering funds associated with criminal activities.
- The Bank will not establish or continue relationships with customers whose conduct gives rise to suspicion of involvement with illegal activities. Any customer relationship where the customer's conduct gives the Bank reasonable cause to believe or suspect involvement with illegal activities, will be reported by the MLRO to the FID and the CBB.

3.1 List of prohibited industries

In line with Burgan Bank's AML Policy, UGB will not open accounts or process transactions for any customer who operates in the following industries:

- Arms, Defense and Military Sector
- Bitcoin or equivalent services / virtual currency or asset provider
- Cargo shipping
- Casinos
- Crowdfunding / Crowdsourcing internet based form of value transfer between donors and recipients)
- Embassies and/or consulates
- Exchange houses
- Internet / Online gambling companies
- Non profit organizations
- Precious metals and stones
- Shell Banks
- Shell Companies
- Social Media Influencers
- Traders in dual use goods (goods that can be used for civil and military purposes)

3.2 UGB's AML Control Procedures for customers

3.2.1 The Bank will implement internal procedures and customer due diligence measures to establish and verify the identity of its customers and their source of funds when:

- Onboarding i.e., establishing business relations and opening an account for a new customer.
- A change to the signatory or beneficiary of an existing account or business relationship is made.

- There is a change in the ownership of the entity.
- A significant transaction takes place.
- There is a material change in the way that an account is operated or in the manner in which the business relationship is conducted.
- Customer documentation standards have changed substantially.
- The Bank has doubts about the veracity or adequacy of previously obtained customer due diligence information.
- Carrying out wire transfers irrespective of value and/or amount that are not consistent with the nature of business.
- There is a suspicion of Money Laundering or terrorist financing.[15]

3.2.2 Proper information will be obtained on the purpose and intended nature of the business relationship, prior to opening the account. [16] Should there be any restrictions imposed on the operation of the account due to the customer being a non-resident, this will be documented in a side-letter between UGB and the customer. The Bank's responsibilities include ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of the relationship, to ensure that the transactions being conducted are consistent with the customer's risk profile/ business profile. [17] This is done by the MLRO/ Deputy MLRO reviewing the daily journal of transactions to review transactions.

3.2.3 The Bank will obtain a written signed statement in hard copy or through digital means from all new customers confirming whether the customer is acting on their own behalf or not. This undertaking is part of the KYC (for individuals/ entities) which is signed by the customer and must be obtained **prior** to opening an account or conducting any transactions with the customer concerned. [18]

3.2.4 Where a customer is acting on behalf of a third party (e.g. Power of Attorney or judicial order), the Bank will also obtain a signed statement from the third party, confirming they have given authority to the customer to act on their behalf. Where the third party is a legal person, the Bank must procure a copy of the original Board resolution (or other applicable document) authorizing the customer to act on the third party's behalf and retain a certified copy. [19]

3.2.5 The Bank will establish and verify the identity of the customer and (where applicable) the party/parties on whose behalf the customer is acting, including the Beneficial Owner of

15 FC 1.1.1; FC 1.1.2. AML 1.1.2

16 FC 1.1.2A

17 FC 1.1.2B

18 FC 1.1.5

19 FC 1.1.6

the funds. [20] It is mentioned in the KYC forms that if the customer is acting on behalf of others, they should be named and the ultimate beneficial owner's identification should be maintained on file.

3.2.6 UGB normally does not provide financial services to a minor or other person lacking full legal capacity. Any exception requires the prior approval of the CEO. After this is procured, the normal identification procedures and KYC due diligence will be conducted on the party operating the account. In the case of minors, the Bank will additionally verify the identity of the parent(s) or legal guardian(s). Where a third party on behalf of a person lacking full legal capacity wishes to open business relations, the Bank will establish the identity of that third party (e.g., Law Firm), as well as the person conducting the business (specific lawyer). [21]

3.2.7 The Bank is prohibited from establishing or keeping anonymous accounts or accounts in fictitious names. Where the Bank maintains a nominee account, which is controlled by or held for the benefit of another person, the identity of that person must be disclosed to the Bank and verified by it in accordance with the requirements specified by the CBB. [22] The opening of nominee accounts (if any), must have the prior approval of the CEO.

3.2.8 UGB will not commence a business relationship or undertake an occasional transaction (above the threshold) with a customer before completion of the relevant CDD measures specified. This includes the risk profiling of the customer. Any restrictions or conditions placed on the operation of the account as a result of the risk assessment, must be communicated to the customer.[23] Verification may be completed after receipt of funds in the case of non-face-to-face business, or the subsequent submission of CDD documents by the customer after initial customer due diligence is completed, providing that no disbursement of funds takes place until the entire CDD is completed. [24]

The process will be as follows:

- Operations is notified about the name of the account that needs to be opened. The unit requesting the opening of account must provide preliminary information pertaining to:
  - Valid Official / Government documents comprising Passport and civil ID in the case of individuals
  - Valid Official / Government documents comprising the Commercial Registration or Certificate of Incorporation, Articles of Association as well as complete ownership structure including the name of the Ultimate Beneficial Owners in the case of entities.

20 FC 1.1.7

21 FC 1.1.8

22 FC 1.1.9

23 FC 1.1.15

24 FC 1.1.10

- Operations will notify the MLRO in advance of the required date of the account opening. The above preliminary information will be forwarded to the MLRO on a timely basis to perform due diligence measures.

- The MLRO will screen the customer, check the country of residency and complete the risk profile based on the process documented in Section #9. Risk based approach (RBA). This includes completing the Worldcheck screening on the name of the proposed account holder and the ultimate beneficial owners. The FATF website (https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions) will be checked to identify whether the country of the customer account is classified as a country with strategic deficiencies or sanctions. Any concerns raised during the initial due diligence will be documented by the MLRO as part of her onboarding review and submitted to the CEO for approval. This is part of the systems and measures that are undertaken to determine the risks of the jurisdiction for each non-resident customer.[25]

- Once this is cleared, Operations will procure the necessary documents required for completing the KYC as mentioned in Section 4 and 5 of this PPM. These will be stored as a soft copy in the UGB Customer Database.

Hard copies of the above will be stored by Operations in the customer files.. Further details are mentioned in Section 6 of this PPM. The MLRO will review the customer database when the file is complete and as part of the Annual MLRO reviews.

3.2.9 Where UGB is unable to comply with the requirements specified by the CBB, it will consider whether to freeze any funds received and file a suspicious transaction report or terminate the relationship or not proceed with the transaction. If the Bank decides to proceed with the transaction (to avoid tipping off the customer), it can consider whether it should file a Suspicious Transaction Report[26]. All three scenarios require the prior approval of the CEO.

3.2.10 In all cases (individuals and entities), UGB will procure the customer's signature on the Terms & Conditions governing the operation of the account. This will document any services which may be restricted or otherwise limited, as a result of the non-resident status.[27]

3.2.11 UGB will not accept non resident customer accounts for companies under formation.

25 FC 1.1.2F

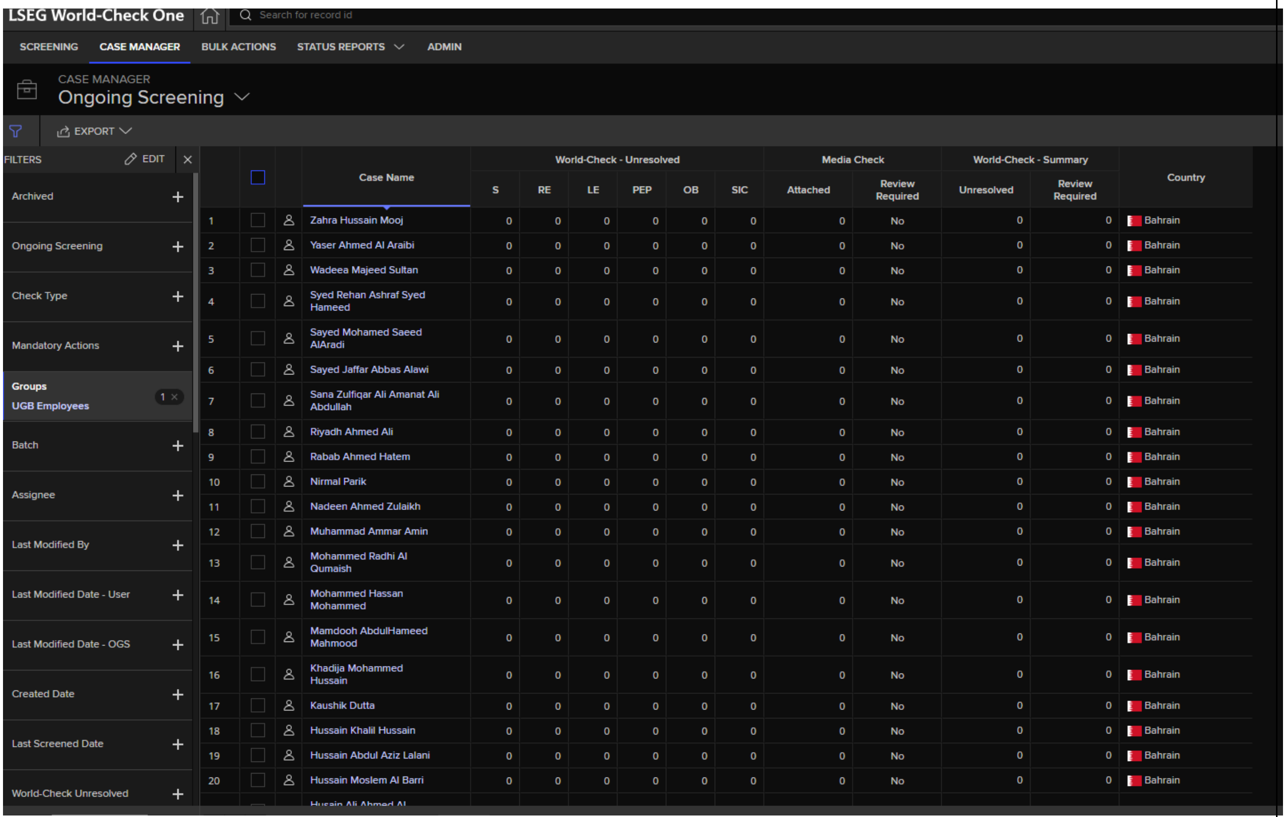
26 FC 1.1.11; FC 5.2.6

27 FC 1.1.15

3.3 UGB's AML Control Procedures for employees

The CBB also requires adequate screening procedures to ensure high standards when hiring employees. [28] These are expected to include controls to prevent criminals or their associates from being inadvertently hired by banks. As the responsibility of all hiring procedures is that of the Human Resources Department (HRD), it is their responsibility to ensure that the Bank obtains a good conduct certificate from the Ministry of Interior prior to hiring any Bahraini employee.[29] The MLRO will also be requested by HR to provide a Worldcheck (screening tool) to run a background check on the prospective employee,. [30]

Good practice also recommends the periodic screening of existing staff to manage the risk of inappropriate behavior in case of changes in their financial circumstances. UGB's MLRO has created a Group in Worldcheck called 'UGB employees'. This list contains the official names of all the Bank's staff and is updated whenever there are resignations or new joiners. Apart from screening the employee name when he/she is hired, the names of employees in this Group are screened by the MLRO annually by switching on the 'Ongoing Screening' toggle, to discern whether there are any matches. Once the exercise is completed, the 'Ongoing Screening' toggle is switched off.



	Case Name	World-Check - Unresolved S	RE	LE	PEP	OB	SIC	Media Check Attached	Review Required	World-Check - Summary Unresolved	Review Required	Country
1	Zahra Hussain Mooj	0	0	0	0	0	0	0	No	0	0	Bahrain
2	Yaser Ahmed Al Araibi	0	0	0	0	0	0	0	No	0	0	Bahrain
3	Wadeea Majeed Sultan	0	0	0	0	0	0	0	No	0	0	Bahrain
4	Syed Rehan Ashraf Syed Hameed	0	0	0	0	0	0	0	No	0	0	Bahrain
5	Sayed Mohamed Saeed AlAradi	0	0	0	0	0	0	0	No	0	0	Bahrain
6	Sayed Jaffar Abbas Alawi	0	0	0	0	0	0	0	No	0	0	Bahrain
7	Sana Zulfiqar Ali Amanat Ali Abdullah	0	0	0	0	0	0	0	No	0	0	Bahrain
8	Riyadh Ahmed Ali	0	0	0	0	0	0	0	No	0	0	Bahrain
9	Rabab Ahmed Hatem	0	0	0	0	0	0	0	No	0	0	Bahrain
10	Nirmal Parik	0	0	0	0	0	0	0	No	0	0	Bahrain
11	Nadeen Ahmed Zulaikh	0	0	0	0	0	0	0	No	0	0	Bahrain
12	Muhammad Ammar Amin	0	0	0	0	0	0	0	No	0	0	Bahrain
13	Mohammed Radhi Al Qumaish	0	0	0	0	0	0	0	No	0	0	Bahrain
14	Mohammed Hassan Mohammed	0	0	0	0	0	0	0	No	0	0	Bahrain
15	Mamdooh AbdulHameed Mahmood	0	0	0	0	0	0	0	No	0	0	Bahrain
16	Khadija Mohammed Hussain	0	0	0	0	0	0	0	No	0	0	Bahrain
17	Kaushik Dutta	0	0	0	0	0	0	0	No	0	0	Bahrain
18	Hussain Khalil Hussain	0	0	0	0	0	0	0	No	0	0	Bahrain
19	Hussain Abdul Aziz Lalani	0	0	0	0	0	0	0	No	0	0	Bahrain
20	Hussain Moslem Al Barri	0	0	0	0	0	0	0	No	0	0	Bahrain

If the match is positive and Worldcheck cites reasons for the match (eg. Lawsuits, misappropriation of funds etc.), the MLRO will escalate the matter to the Head of Human

[28] HC B.2.4A

[29] FC 6.1.6A

30 FC 6.1.6

Resources with a copy to the CEO. The extract from Worldcheck should be forwarded to both of them as an audit trail. The Head of Human Resources will then follow the necessary steps of interrogating the employee and determining whether there is any breach of the code of conduct that warrants a verbal or written warning or in the worst case, dismissal from employment.

4. Face to Face Business Requirements

4.1 Documents required for AML Purposes

If the customer is a natural Person (e.g. Individual), the Bank will identify the person's identity and obtain and record the following official/ government information (in hard copy or electronic form) [31] before providing any financial services. The following information is available in the KYC forms.

(a) Full permanent address (i.e., the residential address of the customer; a post office box is insufficient).

(b) Date of birth.

(c) Place of birth.

(d) Nationality.

(e) Passport number (if the customer is a passport holder).

(f) Current CPR or Iqama number (for residents of Bahrain or GCC states) or any other government issued national identification proof.

(g) Telephone/fax number and email address (where applicable).

(h) Occupation or public position held (where applicable).

(i) Employer's name and address (if self-employed, the nature of self-employment).

(j) Type of account, and nature and volume of anticipated business dealings with the Bank.

(k) Signature of the customer(s).

(l) Utility bill / Bank Statement/ Tenancy Agreement or Documentation from a public/governmental authority as proof of address

(m) Source of funds and/ securities.

(n) Reason for opening the account.

(o) FATCA / CRS self-certification and relevant forms (W8 BEN / W8 BEN E/ W9)

4.1.1. Under the CBB's definition, **all non-resident accounts are subject to enhanced due diligence measures**. UGB will not obtain accounts for any natural non-resident person (irrespective of country of residence) through a digital onboarding process. The Bank will hence verify the information by conducting due diligence on only copies of

31 FC 1.2.1

official/government identification documents that contain the requirements mentioned in (a) and (b) below. This should include a clear photograph of the customer:

(a) Confirmation of the date of birth and legal name, by taking a copy of a current valid official original identification document (e.g., birth certificate, passport, CPR or Iqama);

(b) Confirmation of the permanent residential address by taking a copy of a recent utility bill, bank statement or similar statement from a CBB licensee, or some form of official correspondence or official identification card, such as CPR, from a public/governmental authority, and

(c) Where appropriate, direct contact with the customer by phone, letter, or email to confirm relevant information, such as residential address information.[32]

4.1.2. Any document copied or obtained for the purpose of identification verification should be from an original. For customers based in Bahrain or for employees of UGB, an authorized signatory or officer of the Bank can certify the copy and after sighting the originals, can write **’original sighted’**, together with the date and his name and signature. [33]

4.1.3. Identity documents which are not verified by an authorized official of the Bank in original form (e.g. for nonresident customers of Bahrain) should be certified by one of the following from a GCC or FATF member state:

(a) A lawyer

(b) A notary

(c) A chartered/certified accountant

(d) An official of a government ministry

(e) An official of an embassy or consulate.

(f) An official of another licensed financial institution or of an associate company of the licensee.[34]

(g) An authorized signatory or officer of the Bank of the Bank can attest documents on behalf of the nonresident customer which have already been certified in the above manner. He can however do so by using the ‘True Copy of the Original’ stamp (as opposed to Original Sighted).

4.1.4. The individual making the certification will give clear contact details (e.g., by attaching a business card or company stamp). The Bank will verify the identity of the Person providing the certification through checking membership of a professional organization (for lawyers

32 FC 1.2.3

33 FC 1.2.4

34 FC 1.2.5

or accountants), or through checking against databases/websites, or by direct phone or email contact. [35]

4.1.5. If the customer is a legal corporate entity or a legal arrangement such as a trust, the Bank will obtain and record the following information from the KYC form that it obtains from the customer, as well as copies of original identification documents, databases, or websites, in hard copy or electronic form, to verify the customer's legal existence and structure[36]:

(a) The entity's full name and other trading names used.

(b) Registration number (or equivalent)

(c) Legal form and proof of existence

(d) Registered address and trading address

(e) Type of business activity

(f) Date and place of incorporation or establishment

(g) Telephone, fax number and email address

(h) Names of the relevant persons having a senior management position in the legal entity or legal arrangement

(i) Regulatory body or listing body (for regulated activities such as financial services and listed companies)

(j) Name of external auditor (where applicable)

(k) Type of account, and nature and volume of anticipated business dealings with the Bank

(l) Reason for opening the account.

(m) Source of funds[37].

(n) Sanctions Name of the ultimate beneficial owner/s. This is defined by the natural persons who satisfy all or some of the conditions given below:

- Owning or controlling, directly or indirectly, a percentage equal to or exceeding 10% of the capital or voting rights of the Registered Person;
- Where the Registered Person is a legal person owned by another legal person or legal arrangement, then the Ultimate Beneficial Owner is the natural person who is

35 FC 1.2.6

36 FC 1.2.7

37 FC 1.2.7

the ultimate owner of the ownership chain or who exercises effective control over it;

- The ability to make or influence decisions in the Registered Person either directly or through other means such as personal communications or through participation in the financing of the project, family relations or through any kind of contract, arrangement, understanding, relationship or through a hierarchical entity (in the ownership chain of legal entities);

- The natural person who contributes to financing the business of the Registered Person or its assets, or that transactions are made in its favor, even if these contributions are hidden.

- Having direct or indirect control over the operations of the Registered Person through a management agreement, power of attorney or similar instrument.

- Ultimate effective control through a series of ownerships or other means of control other than direct control of a Registered Person;[38]

4.1.6. The information provided must be attested as mentioned in # 4.1.4 and will be verified by obtaining certified copies of the following documents, as applicable (depending on the legal form of the entity):

(a) Certificate of incorporation and/or certificate of commercial registration or trust deed

(b) Partnership agreement

(c) Board resolution seeking banking services or capital market services

(d) Identification documentation of the authorized signatories of the account

(e) Copy of the latest financial report and accounts, audited where possible (audited copies do not need to be certified)

(f) List of Persons authorized to do business on behalf of the company and in the case of the opening of an account, a Board resolution (or other applicable document) authorizing the named Persons to operate the account (resolution only necessary for private or unlisted companies); and

(g) Memorandum and Articles of Association.39 An extract from the Ministry of Industry, Commerce and Tourism's website through the SIJILAT Commercial Registration Portal, or its equivalent in GCC countries, will suffice for the purposes of verifying the Commercial Registration.[40]

38 Article 3, Ministerial Order Number (83) of 2020 Regarding Criteria, Conditions and Rules Governing the Disclosure of Ultimate Beneficial Owner

39 FC 1.2.8
40 FC 1.2.9A

(h) The names, country of residence and nationality of Directors or partners. [41]

4.1.7. To the extent where no natural person exerts control over the legal person or arrangement, the identity documents of the relevant natural person who holds the position of the senior managing official should be obtained[42]

4.1.8. The Bank will also obtain and document the following due diligence information:

(a) Enquire as to the structure of the legal entity or trust sufficient to determine and verify the identity of the ultimate beneficial owner of the corporate, funds or Securities, the ultimate provider of funds or Securities (if different), and the ultimate controller of the funds or Securities (if different)

(b) Ascertain whether the legal entity has been or is in the process of being wound up, dissolved, struck off or terminated.

(c) Obtain the names, country of residence and nationality of Directors or partners (only necessary for private or unlisted companies)

(d) Get the Sanctions Questionnaire

(e) Procure through new customer documentation or other transparent means, updates on significant changes to corporate ownership and/or legal structure!

(f) Obtain and verify the identity of shareholders holding **10% or more of the issued capital** (where applicable). This information should be entered into the 'Ownership Details' section of the Customer Summary Sheets. Although the requirement to verify the identity of these shareholders does not apply in the case of FATF/GCC listed companies, it is UGB's policy to ensure that due diligence is complete on all its customers to the extent possible.

(g) In the case of trusts or similar arrangements, establish the identity of the settlor(s), trustee(s), and beneficiaries (including making such reasonable enquiries as to ascertain the identity of any other potential beneficiary, in addition to the named beneficiaries of the trust); and

(h) Where a Bank has reasonable grounds for questioning the authenticity of the information supplied by a customer additional due diligence will be conducted to confirm the above information. [43]

41 FC 1.211
42 FC 1.2.8A
43 FC 1.3.1

5. Non resident customers

5.1 Under the terms of its license as a wholesale bank, UGB is permitted to deal only with non-residents of Bahrain. Conventional wholesale banks are permitted to transact with residents of Bahrain and/or in Bahrain Dinar, with respect to taking deposits or providing credit, only where the individual transaction is BD 7 million or above (or its foreign currency equivalent).

5.2 It should be noted that the CBB has categorized non-resident customers to be high risk. Each non-resident customer account will be subject to an **annual review** of enhanced due diligence, a risk scoring, and an MLRO review on the pattern and behavior of movement of transactions in the account.[44] The only exception to this rule is:

	Requirement for enhanced due diligence
Bahrainis and GCC nationals (wherever they reside)[45] (if they are not Politically Exposed Persons)	No

5.3 UGB will not accept any non-resident customers from high risk jurisdictions who are subject to a call for action by the FATF. These are defined as those which are NCCT (Non-Cooperative Countries and Territories) as well as FATF designated countries with strategic deficiencies.[46]

5.4 The Bank will analyze its customer base in terms of geographical distribution on an annual basis.[47] GCC and OECD residents are considered low risk, countries with FATF deficiencies, civil unrest, terrorism, and war are considered high risk, while the rest are deemed to be medium risk. The results of the analysis and the mitigants will be part of the MLRO's annual assessment report to the Board of Directors.

5.5 The Bank will notify customers of any services which may be restricted or otherwise limited, as a result of their non- resident status.[48] This will be on the basis of the results of the risk scoring and risk assessment. [49]

[44] FC 1.1.14,
[45] FC 1.1.17, introduced in September 2023;
[46] FC 1.1.12C
[47] FC 1.1.12D
[48] FC 1.1.15
[49] FC 1.1.10A

6. Enhanced Customer Due Diligence

6.1 General Procedure

6.1.1 Enhanced customer due diligence must be performed by UGB on customers who are deemed to have a higher risk profile. [50] These are defined as***:***

- PEPs (Politically Exposed Persons),
- Customers or entities resident in countries on the FATF's list of Non-Cooperating Countries (NCCT) or countries categorized with strategic deficiencies.
- High net worth individuals and non KIPCO group entities.
- Any individual or entity who has a risk rating of high or extremely high, through the risk scoring process mentioned in Section 9.

6.1.2 Additional queries will be made, or information obtained in respect of the above types of customers. This includes:

- Information on the customer (e.g. Occupation, volume of assets, information available through the public databases, internet etc.) and updating information on the identification data of the customer and the ultimate beneficial owner/s.
- Information on the intended nature of the business relationship
- Information on the source of wealth of the customer
- Information on the reasons for intended or performed transactions (e.g. invoices)
- Approval of senior management to commence or continue the relationship.
- Enhanced monitoring of the business relationship by increasing the number and timing of controls applied and selecting patterns of transactions that require more explanation
- Identifying the source of the first payment in the account and applying RBA
- Evidence of a Person's permanent address using a credit reference agency search or through independent verification by home visit.
- A personal reference (e.g. by an existing customer of the bank)
- Another licensed entity's reference and contact regarding the customer. – the Group Introduction Certificate was introduced by the Bank in 2022.
- Documentation outlining the customer's source of wealth.
- Documentation outlining the customer's source of income; and
- Independent verification of employment or public position held. [51]
- Documentation related to Ultimate Beneficial Owner[52]

6.2 Non-Face to Face Contacts

6.2.1 The Bank follows enhanced due diligence procedures for verifying customer identity where no face-to-face contact takes place.[53] This is to ensure that the customer is the person that they claim to be and to ensure that the address provided is genuinely the customers.[54]

---

50 FC 1.3.1

51 FC 1.3.2

52 Ministerial Order Number (83) of 2020 Regarding Criteria, Conditions and Rules Governing the Disclosure of Ultimate

6.2.2 Where no face-to-face contact takes place, the Bank must take additional measures (in order to mitigate the potentially higher risk associated with such business. These include:

- Telephone contact with the applicant on an independently verified home or business number.
- With the customer's consent, contacting an employer to confirm employment via phone through a listed number or in writing; and
- Evidence of the permanent address using a credit reference agency search.
- Certified copies of bank statements for a recent 3-month period which reflect the salary details.[55]
- Independent verification of employment or public position held. If the account is opened for an employee of any of the Bank's subsidiaries or parent, a letter from the HR Department of the subsidiary confirming employment and the position, should be obtained.
- A personal reference (e.g., by an existing customer of the Bank).
- Another regulated bank from a FATF country or licensed entity's reference regarding the customer.
- Independent and open sources to get more information for the customer risk profile.
- Additional searches for negative news that indicate a financial crime risk profile.
- Evaluating the information provided regarding the destination of funds and the reasons for the transaction.
- Procuring more Information on the intended nature of the business relationship
- Increasing the frequency and intensity of transaction monitoring.

6.2.3 Run a check on the LSEG World Check Service, to ensure the status of any adverse media alerts, or to ensure that the client's name does not appear in any of the "blacklists" issued by various regulatory bodies. A printout giving the findings should be attached to the account opening form. The account holder's name should be input on the World Check system and the relevant box should be ticked to ensure that there is ongoing screening going forward.

6.2.4 The business model of the Bank currently does not include the development and marketing of new products, new business practices, new delivery mechanisms and new or developing technologies for the marketing or support of products. The Bank is however aware that AML risk could be present in investments that it makes in entities. The MLRO will hence conduct a Worldcheck screening on the investee company / loans extended to individuals or corporates and attach this as part of the A rating will also be conducted on the product offered based on the product risk matrix detailed in Section 9.3. This will be documented as an appendix to the Investment Committee / Executive Committee memos[56].

53 FC 1.4.1

54 FC 1.4.2

55 FC 1.4.2,1.4.3

56 FC 1.4.5

6.2.5 As of the date of this manual, no digital onboarding is permitted for any customer.

6.3 Politically Exposed Persons (PEP's) and client acceptance policy for PEPs

6.3.1 PEP is an abbreviation for Politically Exposed Person, a term that describes a person who has been entrusted with a prominent public function, or an individual who is closely related to such a person. These include Heads of State or government, senior politicians, Senior Government, Judicial or Military Officials, Senior Executives of state-owned enterprises, or important political party officials. By virtue of their position and the influence that they may hold, PEPs present a higher risk for potential involvement in unaccounted wealth.

The CBB defines PEPs in Bahrain as Ministers, Members of Parliament, and Ministry officials with the rank of Undersecretary or above. Most financial institutions view such clients as potential compliance risks and perform enhanced monitoring of persons who fall within this category. The requirements for all types of PEPs also apply to family or close associates of such PEPs.[57]

It is important to note at the outset that there is no single and universally agreed definition of PEP. UGB relies on World-Check data to determine their categorization. This can be summarized as follows:

Category	Example
Family	Spouse Partner considered by national law as equivalent to spouse
	Unmarried Partner / cohabitant
	Child or stepchild
	daughter-in-law/son-in-law
	Sibling or step sibling or half-brother / half-sister
	Parent or stepparent
	Parent-in-law / sister-in-law / brother-in-law
	Grandparent and grandchild
Professional and Close Associate	Close Associate or intermediary
	Business Associate / Joint owner
	Private companies / entities / trusts, charities, foundations, or any other onshore / offshore vehicles controlled, 25%+ owned or co-owned by Primary PEP and/or PEP Relative and or PEP associate

At the time of opening the account, UGB staff must use the World Check screening tool to determine whether a customer is a Politically Exposed Person (PEP) or related to one.[58]

57 FC 1.5.3B

58 FC 1.5.1

Other categories of PEPs as specified by the Bank's parent Burgan Bank, are as follows:

Senior Members of the Judiciary	President of the Magistrates Court (Elementary, Appeal, Cassation), Attorney General, Public Prosecutor, Public Defender and their representatives.
Senior Government Officials	Heads of state and government, ministers and governors, heads of government agencies and public bodies and their representatives.
Political Party Officials Members of the Royal Family: Senior Politicians	Party leaders in Arab and foreign countries. Royal Family members in Arab and foreign countries. Speaker of the National Assembly, members of the Executives of state-owned companies and their representatives.
Senior Executives Ambassadors	Executives of state-owned companies and their representatives Senior Diplomats: Ambassador (inside or outside Kuwait).

6.3.2 The Chief Executive Officer's approval must be obtained before a PEP / customer incorporated or resident in a jurisdiction deemed as high risk is accepted as a customer or before his account is closed. [59]

6.3.3 Where an existing customer is a PEP, or subsequently becomes a PEP, enhanced monitoring and customer due diligence measures will include:

(a) Analysis of complex financial structures, including trusts, foundations, or international business corporations.

(b) A written record in the customer file to establish that reasonable measures have been taken to establish both the source of wealth and the source of funds.

(c) Development of a profile of anticipated customer activity, to be used in on-going monitoring.

(d) On-going account monitoring of the PEPs and his/her family or close associates' account by the MLRO. [60] As the names of all PEPs (and other customers) are entered into the Refinitiv World Check database, the MLRO gets email alerts on any media or sanctions related news on the customer. It is his/her responsibility to login to the

59 FC 1.5.2

60 FC 1.5.3, 1.5.4

database and 'clear' the alert by assigning it the Positive/Negative confirmation related to the identity of the customer, and rating the alert in a low/medium/ high risk category. The extracts from Refinitiv World Check on the PEP names also cites the links to family and close associates of the PEPs.

(e) As PEPs fall in the category of high risk, the customer's CDD documentation must be reviewed annually and updated regularly throughout the life of the relationship.[61]

6.4 Enhanced Due Diligence: Charities, Clubs and Other Societies

6.4.1 It is UGB's policy to not open accounts for charitable funds and religious, sporting, social, co-operative, and professional societies. If at all such an account is opened, the Chief Executive Officer's prior approval must be obtained,[62] and the account will be subject to enhanced transaction monitoring by the Bank. The MLRO will develop a profile of anticipated account activity (in terms of payee countries and recipient organizations in particular).[63]

6.5 Enhanced Due Diligence: Pooled Funds

6.5.1 Where UGB receives pooled funds managed by professional intermediaries (such as investment and pension fund managers, stockbrokers and lawyers or authorized money transferors e.g., KAMCO), it will ascertain that the intermediary has applied its usual CDD measures to the identity of the professional intermediary. In addition, UGB will verify the identity of the beneficial owners of the funds where required as mentioned below.[64]

6.5.2 Where funds pooled in an account are not co-mingled (i.e., where there are sub-accounts attributable to each beneficiary), all beneficial owners will be identified by the Bank and their identity verified in accordance with the requirements in Section 5.5.1.[65]

6.5.3 For accounts held by intermediaries where such funds are co-mingled, the Bank will make a reasonable effort (in the context of the nature and amount of the funds received) to look beyond the intermediary and determine the identity of the beneficial owners or underlying clients, particularly where funds are banked and then transferred onward to other financial institutions (e.g. in the case of accounts held for the payment of securities).[66]

Where, however, the intermediary (example KAMCO) is subject to equivalent regulatory and Money Laundering regulation and procedures (and, in particular, is subject to the same due diligence standards in respect of its client base), it is noted that the CBB will not insist upon all beneficial owners being identified, provided UGB has undertaken reasonable

[61] FC 1.1.2C
[62] FC 1.6.1
[63] FC 1.6.3
[64] FC 1.7.1
[65] FC 1.7.2
[66] FC 1.7.3

measures to determine that the intermediary has engaged in a sound customer due diligence process, consistent with the requirements in section. [67]

6.5.4 For accounts held by intermediaries from foreign jurisdictions, the intermediary will be subject to requirements to combat Money Laundering and terrorist financing consistent with the FATF Recommendations and the intermediary will be supervised for compliance with those requirements. The Bank will obtain documentary evidence to support the case for not carrying out customer due diligence measures beyond identifying the intermediary. (e.g., KAMCO). The Bank will satisfy itself that the intermediary has identified the underlying beneficiaries and has the systems and controls to allocate the assets in the pooled accounts to the relevant beneficiaries.

6.5.5 Where the intermediary is not empowered to provide the required information on beneficial owners (e.g. lawyers bound by professional confidentiality rules) or where the intermediary is not subject to the same due diligence standards referred to above, the Bank will not permit the intermediary to open an account or allow the account to continue to operate, unless specific permission has been obtained in writing from the CBB. [68]

6.6 Enhanced Due Diligence: Correspondent Banking Relationships

UGB does not maintain or open correspondent accounts for any third party. [69] UGB however undertakes due diligence on Treasury counterparties with whom the Bank has an active money market and foreign exchange relationship and maintains soft copies of their identity documents.

6.7 Introduced Business from Professional Intermediaries

6.7.1 As normal practice, UGB does not accept maintaining customers introduced to it by professional intermediaries. If at all such customers are introduced, the Bank still has the responsibility of ensuring that the account opening forms, underlying client identification documents and the KYC is maintained for each account that it opens.[70]

6.7.2 The Bank will only accept introduced business if all the following conditions are satisfied:

(a) The customer due diligence measures applied by the introducer are consistent with those required by the FATF Recommendations.

(b) A formal agreement is in place defining the respective roles of the Bank and the introducer in relation to customer due diligence measures. The agreement will specify that the customer due diligence measures of the introducer will comply with the FATF Recommendations.

67 FC 1.7.3

68 FC 1.7.5

69 FC 1.8.1

70 FC 1.9.1

(c) The introducer is able to provide all relevant data pertaining to the identity of the customer and beneficial owner of the funds and, where applicable, the party/parties on whose behalf the customer is acting; also, the introducer has confirmed that the Bank will be allowed to verify the customer due diligence measures undertaken by the introducer at any stage; and

(d) Written confirmation is provided by the introducer confirming that all customer due diligence measures required by the FATF 40+9 Recommendations have been followed and the customer's identity established and verified. In addition, the confirmation will state that any identification documents or other customer due diligence material can be accessed by the Bank and that these documents will be kept for at least five years after the business relationship has ended.[71]

6.7.3 The Bank will perform periodic reviews ensuring that any introducer on which it relies follows the FATF Recommendations. Where the introducer is resident in another jurisdiction, the Bank will also perform periodic reviews to verify whether the jurisdiction is following the FATF Recommendations.[72]

6.7.4 Should the Bank not be satisfied that the introducer follows the requirements of the FATF Recommendations, the Bank will not accept further introductions. It will also discontinue the business relationship with the introducer.[73]

6.8 Enhanced Due Diligence: Shell Banks

6.8.1 It is UGB's Policy to NOT establish business relations with banks which have no physical presence or 'mind and management' in the jurisdiction in which they are licensed ('shell banks') and which are unaffiliated with a regulated financial group. The Bank will not knowingly establish relations with other Bank or financial institutions that have relations with shell banks. There are no exceptions to this.[74]

6.8.2 UGB will immediately file a Suspicious Transaction Report to the Compliance Directorate[75] of the CBB if they are approached by a shell bank or an institution, they suspect of being a shell bank.

6.9 Enhanced Due Diligence: Cross Border Cash transactions.

UGB does not accept any cash transactions. There are no exceptions to this.[76]

71 FC 1.9.2

72 FC 1.9.3

73 FC 1.9.4

74 FC 1.10.1

75 FC 1.10.2

76 FC 1.10A.1-A.3

6.10 Prevention of transfer to digital wallets, crowdfunding, and crypto exchanges

In recent years alternative payment technologies have generated widespread public and investor interest in digital wallets and cryptocurrency. These technologies could potentially create a conduit for money laundering, financing terrorism and evading international sanctions. UGB will not accept any requests from its customers to transfer or receive money to/from digital wallets, crowdfunding sites cryptocurrency exchange houses, digital forensics and incident response (DFIR) companies or digital currency exchanges.

7. Storage and Security of Customer Data

The rules of the CBB require banks to identify and verify individual customers and beneficial ownership of legal entities, understand the nature and purpose of the relationship with the customer opening the account, conduct screening on an ongoing basis to ensure that there is no breach of sanctions and document risk assessment based on the dimensions of nature of customer, geographical residence, type of products/services used and channel of communication. This is based on personal, sensitive data collected from the customers and other documents related to account opening. Hard copies of such information are stored in the individual customer files which are kept securely by the Operations Department. The soft copy of the information is scanned and stored in the UGB Customer Database path in the Publish folder.

The UGB Customer database has information on active and closed clients – these are further bifurcated in terms of individuals, corporate customers and financial institutions. Each folder contains information on:

- Account Opening Forms
- Authorised signatories
- Audited/ reviewed Financials (in the case of entities)
- Board Resolutions and List of Board Members
- Correspondence with the client
- Documentation Checklist
- FATCA and CRS information
- Incorporation documents (CR, Articles & Memorandum of Association, Certificate of Incumbency, Certificate of Good Standing)
- KYC forms
- MLRO reviews and risk rating
- I Identification documents
- Workings on identification of the Ultimate Beneficial Owner/s
- Worldcheck screenings

Other account opening related terms and conditions, fax and indemnity, proof of address, beneficial ownership structure, and other supporting documentation that is required from a regulatory perspective.

A separate register is maintained by the MLRO that provides a synopsis of the status of documentation and the date of the last customer review.

The Personal Data Protection Law of the Kingdom of Bahrain, requires the bank to ‘apply technical and organizational measures capable of protecting data against unintentional or unauthorized destruction, accidental loss, unauthorized alteration, disclosure or access, or any other form of processing. These measures must be capable of providing an appropriate level of security. In order to ensure security and data privacy, access to the folder and the system is restricted to the MLRO, Deputy MLRO, and staff in the Compliance, Internal Audit and Operations Departments.

8. Simplified Customer Due Diligence

8.1 UGB may opt to apply simplified customer due diligence measures if:

(a) The customer is the Central Bank of Bahrain (CBB), the Bahrain Bourse, or a licensee of the CBB.

(b) The customer is a Ministry of a GCC or FATF member state government, a company in which a GCC government is a majority shareholder (e.g. ALBA), or a company established by decree in the GCC (Burgan Bank)[77]

(c) The customer is a company listed on a GCC or FATF member state stock exchange with equivalent disclosure standards to those of the Bahrain Bourse.

(d) The customer is a financial institution whose entire operations are subject to AML/CFT requirements consistent with the FATF Recommendations/Special Recommendations and it is supervised by a financial services supervisor in a FATF or GCC member state for compliance with those requirements.

(e) The customer is a financial institution which is a subsidiary of a financial institution located in a FATFA or GCC.

(f) The customer is a borrower in a syndicated transaction where the agent bank is a financial institutions whose entire operations are subject to AML/CFT requirements, and it is supervised by a financial services supervisor in a FATF or GCC member state for compliance.

8.2 For customers falling under categories (a) and (f) of the above, the customer's name and contact information should be recorded with all other pertinent information. However, if the transaction leads to any cause for suspicion, then as a matter of prudence the Bank will verify identification documentation with respect to customers under this category. [78]

8.3 If and when UGB applies for simplified due diligence measures, it will retain documentary evidence supporting its categorization of the customers. Pertinent documentary evidence may include printouts from a regulator's website, confirmations of the licensed status of the institutions and internal papers attesting to a review of AML/CFT measures applied in a jurisdiction. [79]

8.4 Authenticated SWIFT messages may be used as a basis for confirmation of the identity of a financial institution where it is dealing as principal. For customers who are subsidiaries, UGB will also obtain and retain a written statement from the parent institution of the

[77] FC 1.11.1

[78] FC 1.11.2

[79] FC 1.11.4, FC 1.11.5

subsidiary concerned, confirming that the subsidiary is subject to the same AML/CFT measures as its parent. [80]

8.5 Simplified customer due diligence measures will not be applied where UGB knows, suspects, or has reason to suspect, that the applicant is engaged in Money Laundering or terrorism financing or that the transaction is carried out on behalf of another Person engaged in Money Laundering or terrorism financing. [81]

8.6 The Bank will not apply simplified customer due diligence measures in situations where it has identified high AML / TF/ PF risks.[82]

8.7 The Bank will take reasonable care to establish and maintain appropriate systems and controls for compliance with the requirements of the CBB with respect to anti money laundering, and to limit their vulnerability to financial crime. It will be Bank's MLRO responsibility to document all decisions to do simplified due diligence in any case and to have the decision annually reviewed by the Board and will be available upon request to the CBB. [83]

80 FC 1.11.6
81 FC 1.11.7
82 FC 1.11.7A
83 FC 2.1.1

9. Risk based approach (RBA)

The CBB requires banks to implement a **risk based approach** in establishing its AML/CFT/CPF program and conduct ML/ TF and PF risk assessments prior to, and throughout the course of its relationship with the customer.[84] It has to establish policies, procedures, tools, and systems commensurate with the size, nature and complexity of its business operations to support its RBA.[85] This involves undertaking measures to identify, assess, monitor, manage and mitigate the AML/ TF / PF risks to which the Bank is exposed.[86] The risk assessment has to be properly documented, updated and communicated to the Board of Directors and Senior Management, so that they are aware of the vulnerabilities.[87]

The Board of Directors approves the following risk matrix that is used to develop a risk score for UGB's customers, at the time of onboarding and on an ongoing basis. The score takes into consideration quantitative and qualitative information obtained from relevant internal and external sources. The risk score will be documented by the MLRO at the time of her analysis as specified in Section 13.1 – Annual Compliance Review to the CBB.

The five dimensions used to develop the risk score for customer profiling are based on:[88]

- Customer/investor risk
- Country/ Geographic risk
- Product / service transaction risk
- Distribution Channel risk
- Counter Proliferation Financing (CPF) / Financing of weapons of mass destruction risk

The classification and the risk score assigned by each of the categories specified by the CBB, is expanded below. A score of 1 is Low Risk, 2 is Medium Risk and 3 is High Risk

9.1 Customer / investor risk[89]

	Category	**Score**
1	Individual / Entity is a non-resident	3
2	Individuals / Entities with a net worth of < 1 million	1
3	Individuals / Entities with a net worth of > 1 Million	3
4	Entity is a regulated financial institution.	1
5	Individuals/ Entities are categorized as politically exposed persons (PEPs)	3
6	Individuals/Entities have been sanctioned by the UN, EU, OFAC or any other regulatory body.	3

84 FC-C1.1
85 FC-C1.2
86 FC-C2.1
87 FC-C.2.3
88 FC C.2.3
89 FC C.2.6

7	STRs have been filed by UGB on the activity of the individual/entity.	3
8	Individuals/Entities have a negative history in World check / public sources.	3
9	Individuals / entities establish a relationship with UGB under unusual circumstances (e.g. significant unexplained geographic distance between the financial institution and the customer).	3
10	Individuals/Entities have arrangements to be personal asset-holding vehicles or operate the account on behalf of a third party.	3
11	Individuals/Entities have nominee shareholders or shares in bearer form.	3
12	Entities have a non-transparent ownership structure.	3
13	The ownership structure of the entity appears unusual or excessively complex given the nature of the entity's business.	3
14	Individual / entity is engaged in, or derives wealth or revenues from, a high-risk cash-intensive business	3
15	Individual / Entity's primary source of income originates from high-risk jurisdictions	3

9.2 Country / Geography risk[90]

Country/geographic area risk in conjunction with other risk factors, provides useful information as to potential ML/TF/PF risks. Countries that are identified as being in the international and/or domestic sanctions lists, fall under the 'prohibited category.' (e.g. Iran and Russia). The Worldcheck tool that UGB uses provides alerts on sanctioned countries as it 'monitors over 10,000+ global information resource lists, 900+ sanction, regulatory, law enforcement lists and 5,900+ official/government sites.'[91]

UGB's Board of Directors prohibits the Bank from entering into any relationship regardless of its kind and nature with any individual or entity listed in the international and/ or domestic sanction lists. This includes:

- All transactions to or from prohibited countries, directly or indirectly;
- All business relationships with individuals or entities resident or incorporated, or with primary operations, in prohibited countries;
- All business relationships with entities beneficially owned or controlled by individuals or
  entities based in prohibited countries; and

90 FC C.2.5

91https://www.lseg.com/en/risk-intelligence/search/sanctions-screening?utm_content=Sanctions%20Screening-EME

- All vendor relationships with entities based in any prohibited country.
- If a business or vendor relationship is identified as a prohibited customer, the matter should be escalated to the MLRO
- Regardless of country risk category, relationships and services may be deemed by UGB to be prohibited based on a variety of other factors mentioned in (but not limited to) relevant procedures such as the Customer Risk Assessment Methodology.

In order to assess the geography risk of non prohibited countries, the MLRO will review reports from the website '*Know Your Country.com*'. This paid service collects data from many international and government agencies (FATF, OFAC, EU etc.) and analyses the findings to provide a rating tool that is predominantly focused on money laundering and sanctions issues. The weightages used by '*Know Your Country*'*.com* are currently as follows:

SN	Indicator / Sub Indicator	Weighting %
1	Money laundering/terrorist financing risks	52.5
	1.1. FATF Uncooperative / AML Deficient	*20*
	1.2. FATF Compliance with 40+9 Recommendations	*15*
	1.3. US State ML Assessment	*7.5*
	1.4. US Secretary of State terrorism	*10*
2	International sanctions	15
3	Corruption risks	7.5
4	Global Initiative Criminality Index	10
5	Global Initiative Resilience Index	5
6	EU Blacklist	5
7	Offshore Centre	5
	Total	100%

The Board of Directors recognize that the *Know Your Country* overall scores are a guidance to the Bank's risk weights. A score of > 70 is deemed to be low risk, 65 – 70 is medium risk and < 65 is High Risk. They have however given the authority to MLRO to use a more conservative rating based on her subjective judgement (eg. country is a tax haven).

The MLRO will also review the country risk classification by Burgan Bank while evaluating the geographical risk of UGB's customers. This is shared by Burgan Bank's AFC team on a quarterly basis. The more conservative score between Know Your Country and Burgan Bank's circulated information, will be adopted while assigning the geographical score of the customer.

The approved risk scores are summarized as follows:

Level of Risk	Know Your country score		UGB risk rating
Low Risk	>70	OECD countries	1
High Risk	<65	Non GCC and OECD countries characterized with any one of the following characteristics • civil unrest, war and terrorism • weak governance • part of the FATF / EU list of jurisdictions with strategic deficiencies • US State Department as a Country/Jurisdiction of Primary Concern • Tax haven	3
Medium Risk	65-70	GCC and other countries classified as other than low or high	2

Based on the above matrix, the Board of Directors have approved the following scores that are commensurate with the level of risk:

#	Category	**Score**
1	Customer is resident / incorporated in OECD country	1
2	Customer is resident / incorporated in GCC country	2
3	Customer is resident / incorporated in FATF designated NCCT country or FATF/EU designated country with strategic deficiencies/ non-cooperative jurisdictions for tax purposes	3
4	Customer is resident / incorporated in countries subject to war / civil unrest/ significant corruption/ organized crime/criminal activity.	3
5	Customer is resident / incorporated in countries subject to sanctions	3
6	Customer is resident / incorporated in countries identified as having weak governance, law enforcement and regulatory regimes	3
7	Customer is resident / incorporated in countries with banking secrecy laws that prohibit release of beneficial ownership information	3

The Board of Directors has noted that the certain UGB customers are incorporated in the Cayman Islands and British Virgin Islands - countries which do not provide details on beneficial ownership. As the customers are SPVs which belong to UGB, the Bank has a complete record of its ownership, controllers, and ultimate beneficial owner/s. This risk is hence accepted.

9.3 Product/ Service / Transactions risk[92]

The CBB expects banks to use a risk-based approach to determine the extent to which the offering of its product, service, or transaction, presents potential vulnerabilities to place, layer or integrate criminal proceeds in the financial system. As per best practice, the following are deemed to be high risk products.

- Private banking.
- Anonymous transactions (which may include cash).
- Non-face-to-face business relationships or those sourced through a professional intermediary.
- Products or services that may inherently favor anonymity or obscure information about underlying customer transactions.
- The geographical reach of the product or service offered, such as those emanating from higher risk jurisdictions.
- Products with unusual complexity or structure and with no obvious economic purpose.
- Products or services that permit the unrestricted or anonymous transfer of value (by payment or change of asset ownership) to an unrelated third party, particularly those residing in a higher risk jurisdiction; and
- Use of new technologies or payment methods not used in the normal course of business by the Bank.

The Board of Directors has noted and accepted the following risk scores for products and services/that the Bank offers

	Category - Product	**Score**
1	Assets under custody	2
2	Brokerage	2
3	Deposits and money market placements	2
4	Investments	2
5	Loans	1
6	Trade Finance	3

9.4 Distribution / Channel Risk

The Board of Directors has noted and accepted the following risk scores for distribution / channels [93]:

92 FC C.2.6 and Ff 2.2.7
93 FC C.2.6 and FC 2.2.7

1	Customer provides Face to face instructions	1
2	Customer provides SWIFT based instructions	1
3	Customer Transactions are authenticated through Test Code	1
4	Customer provides Unauthenticated instructions or non-SWIFT instructions that are provided only on mail, e-mail, phone, fax	3
5	Customer's Non-face-to-face instructions are received from Gatekeepers. These could include intermediaries suspected of criminal activities, located in a country with a weak AML/CFT regime, history of non-compliance with laws or regulations, observed to have weak AML/CFT controls.	3

9.5 Counter Proliferation Financing / Financing of weapons of mass destruction

Counter Proliferation Financing (CPF) refers to the act of funding or providing financial services which are used, either wholly or partially, for the manufacture, acquisition, possession, development or otherwise connected in any way to nuclear, chemical, or biological weapons and their related materials (including Weapon of Mass Destruction (WMD)) and dual-use goods used for non-legitimate purposes. CFP can be multi-faceted and attributed to donations, charities, investments in corporates that manufacture dual use goods, it is predominantly channeled through Trade Finance (TF). TF activities in particular require greater scrutiny, due to the due to the risk of multiple parties, modes of shipment and underlying goods, being inadvertently used for financial fraud or illegal trade.

It is hence the Bank's obligation to assess whether the goods/shipments done under its TF activities could be used to finance proliferation or weapons of mass destruction. Based on the FATF list of scenarios that could indicate PF / WMD, the e following risk scores will be used for deriving the risk profile for all customers who have TF activities routed through the Bank or who have activities in sanctioned countries which they have disclosed in the Sanctions questionnaire.

1	Customer's transactions involve person or entity in a foreign country of proliferation concern. (North Korea, Iran and Myanmar)	3
2	Customer's transactions involve shipment of goods incompatible with the technical level of the country to which it is being shipped, (e.g., semiconductor manufacturing equipment being shipped to a country that has no electronics industry).	3
3	Customer's transactions involve persons or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws.	3

4	Customer's transactions involve shipment of goods inconsistent with normal geographic trade patterns.	3
5	Customer's transactions involve dual-used goods, proliferation sensitive or military goods.	3
6	Wire instructions or payment are made from or due to parties not identified on the original letter of credit or other documentation.	3
7	Description of goods on trade or financial documentation is non-specific, innocuous or misleading.	3
8	Information on the end-use or final destination of the trade finance transaction is unclear.	3
9	A freight forwarding firm is listed as the product's final destination	3
10	Order for goods is placed by firms or persons from foreign countries other than the country of stated end-user.	3

A score of 0 will be assigned to this dimension for all customers who do not enter into trade finance transactions with the Bank ordo not operate / transact with counterparties in sanctioned countries.

9.6 Customer Risk Score - Risk weighting of the dimensions

The indicators for each dimension discussed above in Sections 8.1 to 8.5 have been chosen based on criteria that includes their relevance, methodology, jurisdiction, coverage, public availability, and the availability of recent data. As with any composite index, each dimension receives a risk weight that is used to derive an overall risk score for the customer. The weightage differs across dimensions, as certain components are more relevant and applicable than others in assessing ML/TF/PF risk.

UGB's Board of Directors agrees that the dimensions of Customer profile and Country/Geography have a higher risk weightage compared to product, distribution and CPF risk. This is because the bank offers limited products, limited channels of distribution (no internet, digital or mobile banking, and has limited trade finance activities. They hence approve the following risk weights that should be used by the MLRO in deriving the customer's overall risk score.

Weighted Risk Score Calculation		**Weightage**
Customer Risk Profile		60%
Geographic Risk Profile		20%
Product Risk Profile		10%

Channel of distribution Risk Profile		5%
Proliferation Financing Risk Profile		5%
Total		100%

The sum of the five individual dimensions is taken to determine an overall risk weighted score. The bands that determine the classification of Low/Medium/High/ Significantly High will be

Score Range	Likelihood	Impact	Rating
1.0-3.0	Unlikely	Minor Impact	Low
3.01-6.0	Moderately likely	Moderate impact	Medium
6.01-7.5	Likely	Major Impact	High
>7.5	Very Likely	**Significant Impact**	**Significantly high**

Example:

UGB opened an account for a high net worth, non-resident customer in 2008. The customer is owned by a PEP and is incorporated in a country that is witnessing war and civil unrest. The entity has placed money with the Bank in a term deposit for 5 years. . UGB receives outward remittance requests by email from the corporate, to send funds through SWIFT to regulated entities. The entity has no trade finance facilities with the Bank.

The weighted average risk score will be as follows.

Weighted Risk Score Calculation	Weightage	Score	Score
Customer Risk Profile (High net worth, non resident, PEP)	60%	9	5.4
Geographic Risk Profile (country characterized by war and civil unrest)	20%	3	0.6
Product Risk Profile (deposit)	10%	2	0.2
Channel of distribution Risk Profile	5%	3	0.15
Proliferation Financing Risk Profile	5%	0	0
Core Score	100%	17	
Aggregate Weighted Risk Score Calculation			**6.35**

Risk Score of the customer = 6.35 = High Risk

It should be noted that all transactions with PEPs or with financial institutions in FATF designated NCCT countries or financial institutions incorporated / domiciled in nations subject to OFAC sanctions or in countries undergoing conditions of war or civil unrest, or known for money laundering will automatically be categorized as high risk, regardless of the result of their assessment.

A customer rating exceeding 6 must have the approval of the CEO to open an account / entity and must be disclosed to the Board of Directors in the annual MLRO assessment. The MLRO's assessment must also be documented in the underlying customer file.

9.7 Customer Risk Score – UGH Counterparties

It should be noted that under the terms of its license, the Company is not permitted to practice investment activities on behalf of others. UGH hence has **no customer related operations or inward / outward remittances on their behalf that involves SWIFT**. The scope of AML review for UGH hence consists of due diligence that is done on all the financial lenders to the company, as they are financial counterparties[94].

Simplified due diligence and a simplified risk matrix is adopted for UGH, as its financial counterparties are :

- A financial institution whose entire operations are subject to AML/CFT requirements consistent with the FATF Recommendations/Special Recommendations and is supervised by a financial services supervisor in a FATF or GCC member state for compliance with those requirements or

- The customer is a financial institution which is a subsidiary of a financial institution located in a FATF jurisdiction or the GCC.

Risk Matrix for UGH

	Level of Risk Rating (Low/Medium/High)		
Dimension	1	2	3
Customer	Regulated financial institution	Regulated Non-bank financial companies [95]	• Money exchangers • Insurance Companies • All Non-Financial Companies
Country	Financial institutions incorporated in OECD country/GCC country/ Listed on a recognized stock exchange	Financial Institutions Incorporated in Non-OECD / Non GCC country/ or which are unlisted	• FIs in FATF designated black list • FIs in nations subject to OFAC sanctions • FIs in nations with war

[94] Financial counterparties fall under the CBB's definition of customer

[95] The World Bank defines a non-bank financial company (NBFC) as 'a financial institution that does not have a full banking license and cannot accept deposits from the public. However, NBFCs do facilitate alternative financial services, such as investment (both collective and individual), risk pooling, financial consulting, brokering, money transmission, and check cashing.

			/ civil unrest / track record of corruption
Products / Services	Loans	• Assets under custody • Brokerage • Deposits • Investments	• Trade Finance
Channel	Face to face instruction / SWIFT based instructions	Non-face-to-face instructions (including mail, e-mail, phone, text, video, fax, internet)	• Non-face-to-face via Intermediaries deemed to be Gatekeepers [96]
Proliferation Financing	Government institutions and Fis in OECD and GCC countries.	• FIs are incorporated in jurisdictions designated by FATF in countries with strategic deficiencies	• FIs are incorporated in jurisdictions designated by FATF in their black list.

The sum of the five individual dimensions is taken to determine an overall score. The bands that determine the classification of Low/Medium/High have been proposed as follows:

Risk rating of customer	**Range**
Low	0-5
Medium	6-9
High	>9

[96] There is no single definition of gatekeepers, but the FATF briefly defines gatekeepers as 'designated non-financial businesses and professions', including lawyers, notaries, real estate agents, trust, casino, accountants, and other independent legal professionals who perform the role of a trusted third party.

10. On-going Customer Due Diligence and Transaction Monitoring

10.1 Emphasis on-going customer due diligence

10.1.1 The originators and beneficiaries of all incoming and outgoing remittances are screened in the London Stock Exchange (LSEG) Worldcheck system by the Operations Department, prior to processing. In the event that there are no matches, they will be processed in the normal course of business. Cases involving any potential matches or circumstances which appear suspicious, must be referred to the MLRO / DMLRO for resolution. This includes transactions which:

- Do not appear to have a clear purpose or which make no obvious economic sense
- Significant or large transactions that are not consistent with the normal or expected behavior of a customer[97]
  A copy of the screening results is appended to the remittance sheets.

10.1.2 If the MLRO/DMLRO has any reason to **not** resolve potential matches, due to regulatory reasons that are cited in the Worldcheck Alerts, it is their responsibility to notify all UGB staff to exercise caution and not process the transaction. A copy of the email explaining the rationale for leaving the alert unresolved, must be documented to the remittance request. Going forward all names associated with such cases will be documented as red flag examples to be accessed by relevant employees and will be highlighted in the year end AML refresher.

10.1.3 The daily journal which records all inward / outward remittances is reviewed by the MLRO/DMLRO to identify significant or abnormal transactions or patterns of activity.[98] Copies of the underlying SWIFT messages and the screenings are attached to the journal.

10.1.4 Over and above the scrutiny of the daily journal, all transactions above BD 6,000 are captured in a monthly transaction report for manual monitoring and review by the MLRO.[99]

10.1.5 The Bank's process includes vetting significant or abnormal transactions and verifying the source of funds for those transactions Furthermore, the Bank will examine the background and purpose to those transactions and document their findings. The Bank will file a Suspicious Transaction Report (STR) if it is unable to verify the source of funds to its satisfaction. [100]

97 FC 2.2.2

98 FC 2.2.1

99 FC 2.2.3

100 FC 2.2.5

10.1.6 The investigations will be carried out by the MLRO (or relevant delegated official). The documents relating to these findings will be maintained for five years from the date when the transaction was completed. [101]

10.1.7 The Bank will monitor instances where there is a significant, unexpected or unexplained change in customer activity. [102]

10.1.8 When an existing customer closes one account and opens another, the Bank will review its customer identity information and update its records accordingly. The reason for the closure and the fresh opening will also be documented. Where the information available falls short of its CDD/KYC requirements, or is missing or out-of-date new information will be obtained and re-verified with the customer. [103]

10.1.9 Reasonable steps will be taken to ensure that the Bank receives and maintains up-to-date copies of the identification documents. All customers will be required to provide up-to-date identification documents in their standard terms and conditions of business, as well as the relevant tax forms for FATCA purposes.[104]

10.1.10The Bank will review and update their customer due diligence information at least every three years. If, upon performing such a review, copies of identification documents are more than 12 months out-of-date, the Bank will take steps to obtain updated copies as soon as possible. [105]

10.2 Fraud

10.2.1 The CBB requires all its licensees to must ensure that they allocate appropriate resources and have in place systems and controls to deter, detect, and record instances of fraud or attempted fraud.[106] Any potential or actual incidents of fraud should be highlighted to the Chief Audit Executive.

10.2.2 The CCO/ MLRO should report any actual or attempted fraud incident (however small) to the Wholesale Banking Directorate of the CBB and/or any other appropriate authorities (including the CBB)

[101] FC 2.2.6

[102] FC 2.2.7

[103] FC 2.2.8

[104] FC 2.2.9

[105] FC 2.2.11

[106] AML 12.1.1

11. Electronic Transfers

11.1 Outward Transfers & Originating Bank

11.1.1 The Bank will include all required originator information and required beneficiary information details with the accompanying electronic transfers of funds, which is done through SWIFT. This includes:

- the name of the originator.
- the originator's account number or IBAN where such an account is used to process the transaction
- the originator's address, or customer identification number
- the name of the beneficiary
- the purpose codes.
- the beneficiary account number where such an account is used to process the transaction.
- the purpose of the payment[107]

11.1.2 All records of the above information on originator and beneficiary will be maintained by Operations.[108]

11.1.3 No outward remittance will be processed by UGB in its capacity of originating bank if the above information in 10.1.1 is not available.

11.1.4 It is mandatory for Operations to screen the beneficiary in Worldcheck, to ensure that funds are not being remitted to a sanctioned party. If the beneficiary is designated as a PEP, this should be raised to the MLRO and sufficient documentation supporting the remittance should be attached to the outward SWIFT. This includes invoices / loan documents / other communication which supports the purpose of the payment

11.2 Inward Transfers

11.2.1 The Bank will review all inward transfers to ensure that there is adequate originator information. This includes:

- the name of the originator.
- the address of the originator
- the originator's account number or IBAN, or customer identification number
- the name of the beneficiary
- the beneficiary account number where such an account is used to process the transaction.

107 FC 3.1.1; FC 3.1.11
108 FC 3.1.12

11.2.2 In the event that the above information is lacking, the Operations staff should contact the originating institution for the missing information and ask them to supply this within two business days.

11.2.3 If the missing information is not received, Operations should notify the MLRO of the incident, who in turn will review the information and try and contact the originating bank. If no answer is forthcoming, the MLRO will determine the possibility of filing an STR. [109]

11.3 Cross Border Transfers

11.3.1 Most of UGB's transactions fall in this category. While processing such transactions, the Bank will ensure that the information accompanying the wire transfers, includes.

- the name of the originator.
- the originator's address / customer identification number
- the originator's account number or IBAN where such an account is used to process the transaction, or a unique identifier.
- the name of the beneficiary
- the beneficiary account number where such an account is used to process the transaction. [110]

11.4 Domestic Transfers

11.4.1 While processing such transactions, the Bank will ensure that the information accompanying the wire transfers, includes

- the name of the originator.
- the originator's account number or IBAN where such an account is used to process the transaction, or a unique identifier.
- the originator's address, or customer identification number
- the name of the beneficiary
- the beneficiary account number where such an account is used to process the transaction. [111]

11.5 Intermediary Bank

11.5.1 In cases where UGB acts as an intermediary capacity within a chain of wire transfers, Operations has to ensure that all originator and beneficiary information accompanying a wire transfer, is retained in its records. [112]

11.5.2 Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer, a record will be kept, for at least five years, by

109 FC 3.1.4
110 FC 3.1.5, FC 3.1. 6
111 FC 3.1.8
112 FC 3.1.14,

UGB of all the information received from the originating bank or another intermediary bank.[113]

11.5.3 Operations will take reasonable measures to identify cross border wire transfers that lack required originator or required beneficiary information and make an effort to procure the needed information. If this is not available, the MLRO should be informed, so that a decision can be taken as to whether to execute, reject or suspend a wire transfer lacking the underlying information.[114]

11.6 Beneficiary Bank

11.6.1 In cases where UGB acts as a beneficiary bank, Operations has to ensure that all originator and beneficiary information accompanying a wire transfer, is retained in its records.[115]

11.6.2 Operations will take reasonable measures to identify the identity of the beneficiary for all inward transfers. Efforts will be made to procure the required originator or required beneficiary information, in wire transfers where this is lacking. If this is not available, the MLRO should be informed, so that a decision can be taken as to whether to execute, reject or suspend a wire transfer lacking the underlying information.[116]

11.7 Money or Value Transfer Service (MVTS) Provider

11.7.1 Under no circumstances will UGB act as a MVTS Provider, by accepting cash from customers and making a payment of a corresponding sum in cash (e.g. Western Union).[117]

113 FC 3.1.15

114 FC 3.1.18, FC 3.1.19

115 FC 3.1.20

116 FC 3.1.16, FC 3.1.17

117 FC 3.2.1

12. Appointment of the MLRO

12.1 MLRO

12.1.1 UGB will appoint an MLRO that has a Reporting Line to the Chairman of the Board of Directors, for matters relating to AML. This is a 'controlled position.' The CBB's approval is hence required prior to appointing any person as the MLRO. Any change in the MLRO requires notification to the CBB. [118]

12.1.2 The position of the MLRO will not be combined with functions that create potential conflicts of interest, such as an internal auditor or business line head. It also cannot be outsourced.[119] It can be combined with that of the Compliance Officer as UGB's volume and geographical spread of the business is limited. [120] In any case, when combining the MLRO of the DMLRO position with any other position within the Bank, this will be specified in the Application for Approved Person Status – Form 3.[121]

12.1.3 The Bank will also appoint a Deputy MLRO. This is a controlled function and also subject to the CBB's prior approval. The deputy MLRO will support the MLRO to discharge designated responsibilities and deputize in his absence. [122]

12.1.4 In order to enable the MLRO can carry out his responsibilities effectively, the Bank will ensure that the MLRO:

(a) Is a member of senior management of the Bank.

(b) Has a sufficient level of seniority within the Bank and has the authority to act without interference from business line management and has direct access to the Board and senior management (where necessary).

(c) Has sufficient resources, including sufficient time and support staff, and has designated a replacement Deputy MLRO to carry out the function should the MLRO be unable to perform his duties.

(d) Has unrestricted access to all transactional information relating to any financial services provided by the Bank to that customer, or any transactions conducted by the Bank on behalf of a customer.

(e) Is provided with timely information needed to identify, analyze, and effectively monitor customer accounts.

---

118 FC 4.1.1

119 FC 4.1.2

120 FC 4.1.3

121 FC 4.1.3A

122 FC 4.1.4

(f) Has access to all customer due diligence information obtained by the Bank; and

(g) Is resident in Bahrain. [123]

12.1.5 In addition, UGB will ensure that the MLRO is able to:

(a) Monitor the day-to-day operation of its policies and procedures relevant to this Policy.

(b) Respond promptly to any reasonable request for information made by the Anti Money Laundering Unit, or the CBB. [124]

12.1.6 If the position of the MLRO falls vacant, the Bank will appoint a permanent replacement (after obtaining CBB approval), within 120 calendar days of the vacancy occurring. Pending the appointment of a permanent replacement, the Bank will make immediate interim arrangements (including the appointment of an acting MLRO) to ensure continuity in the MLRO function's performance. These interim arrangements will be approved by the CBB. Any action taken by the acting MLRO will be regarded as having the same authority as if it had been done by the MLRO. [125]

12.2 General Responsibilities of the MLRO

These include:

12.2.1 Establishing and maintaining the Bank's AML/CFT policies and procedures and validating that these are up to date.

12.2.2 Ensuring that the Bank complies with the AML Law, any other applicable AML/CFT legislation.

12.2.3 Ensuring day-to-day compliance with the Bank's own internal AML/CFT policies and procedures. This includes a review of the daily transactions to ensure that screening is done on all beneficiaries. The MLRO also does her own screening in Worldcheck, Mediacheck and /or open sources, in the case of any transactions which require further due diligence or investigation.

12.2.4 Acting as the Bank's main point of contact in respect of handling internal Suspicious Transaction Reports from the Bank's staff and as the main contact for the Financial Intelligence Unit, the CBB and other concerned bodies regarding AML/CFT;

[123] FC 4.1.6

[124] FC 4.1.8

[125] FC 4.1.9

12.2.5 Taking reasonable steps to establish and maintain adequate arrangements for staff awareness and training on AML/CFT matters (whether internal or external).

12.2.6 On-going monitoring of high-risk customer accounts; and maintaining all necessary CDD, transactions, STR and staff training records for the required periods [126]

12.2.7 Conducting a risk assessment of the overall AML program by using key performance indicators as mentioned in Section 10.3

12.2.8 Producing annual reports on the effectiveness of the Bank's AML/CFT controls, for consideration by senior management and the Board of Directors.

126 FC 4.2.1

13. Compliance Monitoring & Reporting Responsibilities of the MLRO

13.1 Annual Compliance Review to the CBB and the Board of Directors

13.1.1 UGB's MLRO will review the effectiveness of its AML/CFT procedures, systems, and controls at least once each calendar year. The scope of the review will include:

(a) A report, containing the number of internal reports, a breakdown of all the results of those internal reports and their outcomes for each segment of the Bank's business, and an analysis of whether controls or training need to be enhanced.

(b) A report, indicating the number of external reports made in and, where a Bank has made an internal report but not made an external report, noting why no external report was made.

(c) A sample test of compliance with this Module's customer due diligence requirements; and

(d) A report as to the quality of the Bank's anti-money laundering procedures, systems and controls and compliance with the rules of a licensed exchange and clearing and depository corporation, AML Law, and this Module. [127] This can be in the form of a compliance assessment of Module FC, in the Risk Nucleus Compliance system.

13.1.2 The reports listed under section 13.1.1 (a) and (b) will be made by UGB's MLRO. The sample testing required under rule section 13.1.1 (c) and the report required under section 13.1.1 (d) will be undertaken either by the Bank/ subsidiaries' external auditors or a consultancy firm approved by the CBB. [128]

13.1.3 The MLRO's annual AML assessment for UGB and UGH will be submitted to the respective Boards for their review and approval. If deemed essential, remedial measures must be commissioned by the Board/s and copied to the Bank's senior management. [129]

13.1.4 The Bank and the subsidiaries will instruct their external auditor to produce the report referred to in section 13.1.1 (c) and (d) and submit the same to the CBB by the 30th of June of the following year. The findings of this review will be received and acted upon by the Bank. [130]

13.1.5 Making external Suspicious Transaction Reports to the Financial Intelligence Unit and the Anti Financial Crime Directorate of the CBB.

127 FC 4.3.1B

128 FC 4.3.2A

129 FC 4.3.3

130 FC 4.3.5

13.2 Annual Risk Review of Customers

The CBB requires Banks to review and update the customers' risk profile based on their level of ML/TF/PF risk upon onboarding and regularly throughout the life of the relationship.[131] This is in line with the risk management and mitigation measures which are commensurate with the nature and size of UGB's business. [132] Apart from the risk scoring undertaken to identify and assess their AML risk for customers are based on the four dimensions of customer profile, countries or geographic areas, products, services, transactions, and delivery channels, the MLRO will also review the bank statements for the previous year. This is to ensure that transactions undertaken throughout the course of the relationship is consistent with the Bank's knowledge of the customer, its business risk and risk profile.[133] Findings should be documented by the MLRO in her annual reviews and reviewed by the external auditor in order to be able to demonstrate that assessments are up to date.

The CBB requires all banks to maintain and regularly review and update the documented risk assessment.[134] The **annual review** of each individual and corporate customer, risk scoring and the enhanced due diligence for customers rated as high risk and significantly high risk must be completed by the MLRO by August of each year. Based on the information stored in the customer database and the secure folder containing customer data, the MLRO scrutinizes the validity and completeness of the existing personal information and documents required for opening the account, as well as the pattern of behavior. This is compared with the anticipated movement of funds as declared in the KYC. The review documents the number and nature of any significant transactions, changes in the way that the bank account is operated or in the manner in which the business relationship is conducted, patterns and behavior and the risk profile at the time of onboarding vis a vis the current risk profile based on the dimensions of nature of customer, country, products/services and channel of communication.

The sources of data for the reviews will be the KYC provided by the customer and

- the FATCA and CRS forms which certify the country of residency.
- the Account Statements provided by the Operations Department which detail the movement of funds.
- Public financials statements and databases,
- Internal and external investment and credit reviews.
- World Check System

The CBB guidelines require specify obtaining the approval of senior management to commence or continue the business relationship.[135] The MLRO's memo documenting the

131 FC 1.1.2C
132 FC 4.3.1
133 FC 2.2.10
134 FC C.1.3

135 FC 1.3.2 (e)

categorization and risk score of UGB's customers, must be signed by the CEO on an annual basis.

13.3 Annual Compliance Review of KPIs for Departments and Staff

The CBB requires all Banks to incorporate Key Performance Indicators (KPIs) to ensure compliance with AML/CFT requirements by all staff.[136] The performance against the KPIs must be adequately reflected in their annual performance evaluation and in their remuneration.

UGB has designed the KPIs on two categories:

- generic that are specific to all staff – these will be included as part of the annual performance evaluation forms.
- department specific. – these will be part of the department specific key performance indicators, which are taken into consideration as part of the remuneration evaluation process.

The KPIs that fall under both categories are:

Generic
• Attendance at the annual AML refresher
• Awareness of raising internal STRs to the MLRO/Department MLRO • Signing the Code of Conduct affirmation that includes the responsibility of raising STRs and having AML awareness

Department Specific KPIs

These KPIs will be filled out by the Department Head at the time of submitting the other KPIs of the department to HR, as part of the remuneration process.

Accounts & Finance

	Low	Medium	High
Number of cheques processed without adequate documentation.	0 – 5	6 -10	>10
Number of instances of not procuring VAT registrations from vendors prior to processing payments	0 – 5	6 -10	>10
Number of instances of not identifying a potentially suspicious transaction /	0 – 3	4 -10	>10

[136] FC 2.1.3

escalating the same to the MLRO			

Asset Management & Investment Banking

	Low	Medium	High
Number of instances of not identifying a potentially suspicious transaction or AML concerns while conducting a due diligence review.	0 – 3	4 -10	>10

Compliance (covers the MLRO function)

	Low	Medium	High
Number of instances of not investigating an internal STR	0	1 - 3	>3
Number of instances of not reporting an STR to the regulators	0	1 - 3	>3
Delay in updating the annual AML PPM (Number of months after one year has elapsed from the date of last BOD approval)	0 -3 months	4 – 6 months	>6 months
Delay in conducting the annual risk assessment of customers. (After 30 June of each year)	0 -3 months	4 – 6 months	>6 months
Delay in submitting the annual assessment of AML to the Board of Directors (After 30 June of each year)	0 -3 months	4 – 6 months	>6 months
Number of AML issues outstanding from internal audit and/or the external auditors' findings	0 – 3	4 -10	>10

Credit & Risk Management

	Low	Medium	High
Number of instances of suspicious transactions identified from the risk grading assigned in 'Risk Approval Forms.'	0 – 1	2 - 3	>4

Number of instances of suspicious transactions identified from the investment reviews.	0 – 1	2 - 3	>4
Delay in conducting the bank and counterparty risk reviews. (Number of months after one year has elapsed from the date of last BOD approval)	0 – 2 months	3 months	>3 months

Human Resources & Administration

	Low	Medium	High
Number of instances of oversight in conducting the background checks of new employees	0 - 3	4 - 5	>5
Number of instances of oversight in arranging AML training for new staff within the stipulated 3-month period.	0 - 3	4 - 5	>5

Internal Audit & Quality Assurance

	Low	Medium	High
Active participation in the annual AML External reviews.	0 - 5	6 - 10	>10
Active follow-up of all AML findings / issues pending implementation.	0 - 5	6 - 10	>10
Number of instances of not independently investigating a STR once brought to the attention of IA.	0 - 3	4 - 5	>5

Operations

	Low	Medium	High
Number of instances of not informing the MLRO/Deputy MLRO on suspicious inward	0 - 5	6 - 10	>10

or outward payments, including 'wire-stripping' i.e., where the source and destination of incoming and outgoing funds have been masked.			
Number of outstanding accounts with missing documentation	0 - 5	6 - 10	>10
Number of outstanding accounts with outdated documentation	0 - 5	6 - 10	>10
Number of instances of not screening customer names and beneficiaries on Worldcheck for all inward and outward wire transfers. (Interbank transfers are excluded)	0 - 5	6 - 10	>10

Treasury

	Low	Medium	High
Delay in providing information for the bank and counterparty risk reviews. (Number of months after one year has elapsed from the date of last BOD approval)	0 – 3	4 -10	>10
Delay in notifying the MLRO/Deputy MLRO of any new interbank counterparty relationships from the date of commencement (number of months)	0 – 1	2 - 3	>3
Delay in providing the MLRO/Deputy MLRO with the list of active Treasury counterparties (after 30 June[137] of each year).	0 – 1	2 - 3	>3

[137] 30 June is considered to be the reference date, as it is the deadline for submission to the CBB of the external auditors' independent external assurance report on adherence to AML rules.

Information Technology

	Low	Medium	High
Number of instances of delay in generating the monthly AML transaction reports	0 – 3	4 - 5	>5
Number of instances of not informing the MLRO/Deputy MLRO on suspicious transactions identified from IT logs.	0 – 3	4 - 5	>5

13.4 Annual Assessment to the BAC and Board of UGB

The MLRO's annual assessment of UGB's AML Framework will cover the following matters:

- Significant Changes in AML Regulations during the past year.
- Synopsis of Internal and External Suspicious Transactions investigated / filed in the previous year.
- Details of other ad-hoc AML related reports submitted to the CBB during the previous year.
- Details of the methodology of the risk based approach adopted by UGB.
- Analysis of customers by profile, geography, product and channel of distribution.
- Vulnerability to terrorism financing / proliferation financing
- Status on KYC documentation
- Key Performance Indicators (KPIs) on AML Performance Indicators
- Statistics N screening
- Statistics on AML Training conducted during the previous year.
- Synopsis of the findings of the Agreed upon procedures report submitted to the CBB on UGB and its financial subsidiaries on the AML Framks. A proposed action plan and the time frame to remedy any pending issues will also be documents.

13.5 Quarterly Compliance Review to the BAC

The MLRO's quarterly report to the BAC will contain a section on AML that covers the following matters:

- AML Staff training (new and existing)
- AML Policy updates
- Suspicious transactions raised internally during the quarter
- Suspicious transactions reported / closed / in progress made to the CBB
- Key AML issues within the quarter
- Any positive matches found in Worldcheck related to names in the sanctioned lists.

13.6 Reporting to Burgan Bank's GAFC

The MLRO's quarterly report to the GAFC will cover the following information requested:

- General inquiries on customers, geography, and products
- Inspections and regulations
- Staffing, Training and Awareness
- Policies and Procedures
- Systems and Watchlists
- On-boarding and review
- Unusual and suspicious activity and transaction

The MLRO will also complete Burgan Bank's annual risk assessment and sanctions assessment every year, using the Association of Certified Antim Money Laundering Specialist (ACAMS) Risk Assessment Tool. This is a lengthy exercise that involves answering a series of questions with the underlying justifications and serves as an additional quality assurance from an Enterprise wide AML Risk perspective and will require the collaboration of other departments like Accounts & Finance and Credit & Risk Management to provide the MLRO/ DMLRO with numerical data on income from customers, volume and value of products/ transactions. Any gaps found in the assessment must be highlighted by the MLRO in her annual assessment to the Board of Directors, along with a proposed action plan to close the shortcomings.

Both assessments must be completed annually within the stipulated deadlines of the GAFC.

13.7 AML controls and responsibilities conducted by other departments of UGB

It is an accepted fact that AML is a collective responsibility of each employee of the Bank. The following table documents the AML controls and processes undertaken by other departments of UGB.

Department	Area of Reliance	Description
Operations	Customer Data Management	• Responsible for gathering, updating, and securely storing customer information used for AML and KYC purposes
	Data Gathering	• Requests and collects customer information to support KYC updates and replace expired data.
	Customer File custody	• Maintains Customer physical files and ensures their AML related data and information are updated on a timely basis.
	KYC Preparation	• Prepares customer profiles, ensuring completeness and accuracy of KYC documentation.
	CBB Blocking System	• Central Bank of Bahrain (CBB) utilizes an online blocking

		system for financial institutions to process blocking orders and inquiry requests efficiently. On a daily basis the Operations department reviews and clears names on the CBB Blocking system.
	Transaction Screening	• Conducts initial screening of transactions for potential AML red flags, performs manual screening of beneficiaries and counterparties using World-Check prior to processing payments.
	Transaction Monitoring for STR	• Overseas daily transactional flows and flags unusual patterns or behaviors
	Escalation of Flagged Activity	• Escalates suspicious or unusual transactions to the MLRO for further review
	Daily report Extraction	• Extracts daily transaction reports from the TCS System and submits them to the MLRO to support ongoing monitoring and review. Arranges with IT Department for ADHOC SWIFT extract reports.
Account & Finance	Annual Customer Cheque Report	• Prepares and provides the annual customer check report to the MLRO
	Cheque Issuance and Review	• Reviews and verifies cheque rationale and reasoning details before processing.
	Custom MIS Reporting	• A monthly report on all cheques issued is provided to the MLRO. A monthly report on all transactions exceeding BD 6,000 is prepared for the MLRO.
Human Resources	Confidential Document Retention	• Retains confidential documents related to individual customers salary and other sensitive information.
	New hire employees	• Conducts background checks on new employees and informs MLRO If any issues were noted during background verification.
Risk	DMLRO	• Acts as the Deputy MLRO and serves as backup to the MLRO.
	SWIFT Relationship Management Application approver	• Acts as a SWIFT Relationship Management Application approver and reviews existing relationships for their activity.

14. Internal reporting

14.1 Suspicious Transactions

14.1.1 A suspicious transaction will often be:

- Any transaction where the amount, duration or other specific feature is inconsistent with the customer's professional or business activities, standard of living or normal movements on the account.
- A transaction that is not logical from an economic, financial, or Banking point of view.
- There is a suspicion of a potential fraudulent transaction or fraudulent remittance instructions.

14.1.2 Examples of what might constitute a suspicious transaction, by activity, are listed below. These are by no means exhaustive and only provide certain basic ways in which money can be laundered.

- Cash transactions.
- pass-through or "in and out" transactions.
- transactions with entities which are not believed to have comprehensive KYC and anti-money laundering policies, and which are incorporated in or have their primary place of business in countries which have inadequate anti-money laws.
- customers whose wealth emanates from activities susceptible to money laundering.
- any unusual financial activity of the customer in the context of his own usual activities.
- any unusual transaction during some usual financial activity.
- any unusually linked transactions.
- any unusual employment of an intermediary during some usual transaction or financial activity.
- any unusual method of settlement.
- any unusual or disadvantageous early redemption of an investment product; and
- any unwillingness by the customer to provide the information requested.

14.2 Internal Reporting of Suspicious Transactions for Staff and Management

It is the duty of every member of management and staff to report any suspicious transactions or suspicions to the MLRO. This includes remittances received for non customers / incorrect inward remittances. Failure to do so could result in disciplinary action.[138]

14.2.1 All Internal Reports must reach the MLRO and must not be blocked. It is reiterated that there should be complete cooperation from all Department Heads with respect to escalating STRs.[139]

138 FC 5.1.1

139 FC 5.1.2

14.2.2 The concerned employee should fully explain the reason for the suspicion Such suspicions must not be discussed with anyone outside the Bank. Care must be taken in discussing a suspicion even with other colleagues. If it is considered appropriate, the discussion must be held only with the MLRO.

14.2.3 It is vital that no mention of such suspicion be made to the customer, the beneficial owner or other subjects of the STR. Any discussion of this nature would risk a **tipping off** offence being committed if the customer became aware that a report had been submitted.[140]

14.2.4 All staff must note that once the reporting process has commenced, it must be followed through and completed even if the original suspicion might appear to have been resolved. Where appropriate, the MLRO will add any comments that provide additional information relevant to the report.

14.2.5 The MLRO will examine all reports and make additional enquiries as deemed appropriate. He / She has full access to all information including KYC information that is in the possession of any department of the Bank. [141] An internal report will be compiled by him/her and maintained in the UGB Customer Database as long with supporting documentation..[142]

14.2.6 This procedure must be followed and repeated every time there is an unusual transaction, even if the Bank has already notified the FID and the CBB of previous unusual transactions relating to that customer/account. This reporting requirement applies regardless of whether the transaction involves tax matters.[143]

14.2.7 If the MLRO opines that there is a fraudulent/ potential fraudulent transaction or incorrect remittance instruction, he/she will immediately escalate the incident to Internal Audit for investigation. In case the incident is affirmed by Internal Audit, the Compliance Department will notify the Wholesale Banking Department of the CBB in accordance with the CBB's requirement to notify them on all frauds.[144]

14.3 Procedures undertaken by the MLRO.

Upon receiving the internal report, the MLRO will undertake sufficient enquiries to determine whether, in his/her judgement the abnormal transaction is suspicious or a sanctions rule is breached.
This could include reviewing the account opening records, KYC information and historical transaction patterns.

The MLRO may wish to discuss the report with:

140 FC 5.2.6

141 FC 5.2.2

142 FC 5.2.1

143 FC 5.2.4

144 BR-5.1.13

- The member of staff.
- The Head of the Department
- The Head of Internal Audit.

All findings will be documented, and copies of the reports submitted to the FIU and the CBB will be retained by him/her. If a decision is made not to report to the FID, a record of the report will be retained along with an explanation as to why the incident was not reported.

14.4 UN Security Council Resolutions

UGB will comply with United Nations Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing. It will freeze, without delay, the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity either (i) designated by, or under the authority of, the United Nations Security Council under or any names that are communicated by the Compliance Directorate or the Financial Stability Directorate of the CBB. [145]

145 FC 8.2.1AA

15. External reporting

15.1 Procedure for External Reporting

15.1.1 The Bank will take reasonable steps to ensure that all reports discussed above in Sections 14 are considered by the MLRO (or his duly authorized delegate). Having considered the report and any other relevant information, if the MLRO (or his duly authorized delegate), still suspects that a Person has been engaged in Money Laundering or terrorism financing, or the activity concerned is otherwise still regarded as suspicious, he/she will report the fact promptly to the Relevant Authorities. Where no report is made, the MLRO will document the reasons why. [146]

15.1.2 To take reasonable steps the Bank will:

(a) Require the MLRO to consider reports in the light of all relevant information accessible to or obtainable by him/her.

(b) Permit the MLRO to have access to any information, including Know Your Customer information; and

(c) Ensure that where the MLRO, or his duly authorized delegate, suspects that a Person has been engaged in Money Laundering or terrorist financing, a report is made by the MLRO which is not subject to the consent or approval of any other Person. [147]

15.1.3 The MLRO's report will go to the Financial Intelligence Directorate at the Ministry of the Interior, with a copy sent to the CBB's AFC Directorate. Reports will be made using the Suspicious Transaction Report (STR) form accessible on the IIS System https://cbbclick.gov.bh. [148]

15.1.4 All suspicious transactions or attempted transactions will be reported promptly to relevant authorities. This reporting requirement applies regardless of whether the transaction involves tax matters. [149]

15.1.5 The Bank will also report to the AFC Directorate, all assets frozen or actions taken in compliance with the instructions of the CBB with respect to their circulars received with respect to United Nations Security Council Resolutions (UNSCR)[150]

146 FC 5.2.1

147 FC 5.2. 2

148 FC 5.2. 3

149 FC 5.2. 3

150 FC 8.2.4 (c)

15.1.5 All relevant details of STRs submitted to the relevant authorities will be maintained by the MLRO for at least years.[151]

16. Reporting to the SRO (Self Regulating Organisation)

This section is applicable only to UGH but is mentioned in this AML PPM in line with the service level agreement signed between the Company and the Bank. If the money laundering offence is related to capital markets i.e. buying or selling of securities, the MLRO shall notify the Bahrain Bourse's Member Affairs Department, alongside the notification sent to the FID and the CBB. It is the responsibility of the Bourse to stop the execution of the suspicious transaction and any security deposited with the Bourse or any other bank.

Email: members@bahrainbourse.com.bh;
Cmsd.compliance@cbb.gov.bh

17. Contacting the Relevant Authorities

Reports made by the MLRO or the Deputy MLRO have to be reported to the Ministry of the Interior and copied to the Compliance Directorate at the Central Bank of Bahrain [152] through the IIS portal https://cbbclick.gov.bh/ and choosing the option for filing STR. The addresses for contact of the regulatory authorities are given below.

Financial Intelligence Directorate

General Directorate of Anti-Corruption and Economic and Electronic Security
Ministry of Interior
P.O. Box 26698
Manama, Kingdom of Bahrain
Telephone: 17 749397
Fax: 17 715502
E-mail: bahrainfid@moipolice.bh

Director of Compliance Directorate

Central Bank of Bahrain
P.O. Box 27
Manama, Kingdom of Bahrain
Telephone: 17 547107
Fax: 17 535673
E-mail: Compliance@cbb.gov.bh[153]

151 FC 5.2.4; FC 5.2.5

152 FC 5.3.1

153 FC 5.3.2

18. Training

18.1 Procedures for Training

18.1.1 It is UGB's parent - Burgan Bank's requirement that all Directors and staff receive an AML refresher every year. Executive Directors of UGB who are Burgan Bank employees automatically receive training from Burgan Bank. It is hence UGB's responsibility to ensure that all independent directors of the Bank, senior management, and staff who handle customer transactions are provided an annual refresher training This will cover:

(a) Their responsibilities under the AML Law, this Module, and any other relevant AML/CFT laws and regulations;

(b) The identity and responsibilities of the MLRO and his deputy;

(c) The potential consequences, both individual and corporate, of any breach of the AML Law, this Module and any other relevant AML/CFT laws or regulations;

(d) The Bank's current AML/CFT policies and procedures.

(e) Money Laundering and terrorist financing typologies and trends.

(f) The type of customer activity or transaction that may justify an internal report in accordance with Section 14 ;

(g) The Bank's procedures for making an internal report and

(h) Customer due diligence measures with respect to establishing business relations with customers. [154]

18.1.2 There is a requirement that new employees must be given AML/CFT training within three months of joining the bank.[155] HR notifies the MLRO of all new employees so that they can be trained on a one-on-one basis within the stipulated three-month period. Such staff are also expected to attend the annual refresher in accordance with the requirement that AML/CFT training should be provided to staff at least once a year. [156]

18.1.3 Attendance by staff in the Asset Management & Investment Banking Department, CRM, Treasury and the Operations Department, is mandatory, as they are responsible for / heavily involved in the opening of accounts / handling of customer transactions. All material used will remain available for reference by staff during their period of employment and can be accessed through the Bank's Intranet under the "training" tab. [157]

154 FC 6.1.1

155 FC 6.1.3

156 FC 6.1.5

157 FC 6.1.2

18.1.4 Both the MLRO and DMLRO will attend a specialized, external training on AML on an annual basis to ensure that he/she foster a well informed and responsive AML culture. It also enables the MLRO to ensure that the content for the AML/CFT training for relevant staff remains up-to-date and is appropriate given the Bank's activities and customer base.[158]

18.1.4 The Bank will conduct AML/CFT training to relevant and new staff at least once a year. This will be followed up with a quiz that provides assurance on their understanding of the Bank's AML framework. A threshold of 70% is considered to be satisfactory. The results of the quiz will be analyzed by the MLRO, to determine employees who require further training. Staff members who do not meet this threshold will be sent to the Bahrain Institute of Banking & Finance to attend an in-depth AML training.

158 FC 6.1.4

19. Record Keeping Requirements

19.1 CDD and Transaction Records

The Bank will comply with the record-keeping requirements contained in the AML Law and in the CBB Law. It will hence retain adequate records (including accounting and identification records), for the following minimum periods:

(a) For customers, in relation to evidence of identity and business relationship records (such as application forms and business correspondence), for at least five years after the customer relationship has ceased; and

(b) For transactions, in relation to documents enabling a reconstitution of the transaction concerned, for at least five years after the transaction was completed. [159]

(c) In accordance with the Capital Markets Supervision Directorate's requirements, proper records that are sufficient to show and explain UGB's transactions and commitments in respect of its client assets related to brokerage, will be retained for a period of a minimum of 10 years after they were made.[160]

19.2 Compliance Records

UGB's MLRO will retain copies of the reports produced for the annual compliance review for at least five years. The Bank will also maintain for five years reports made to, or by, the MLRO by internal staff, along with records that show how these reports were dealt with and what action, if any, was taken as a consequence of those reports. [161]

19.3 Training Records

(a) The Bank will maintain for at least five years records showing the dates when AML/CFT training was given, the nature of the training, and the names of the staff that received the training. [162]

(b) All records required to be kept under this section will be made available for prompt and swift access by the Relevant Authorities or other authorized Persons. [163]

159 FC 7.1.1

160 MIR 4.7.21

161 FC 7.1.2

162 FC 7.1.3

163 FC 7.1.4

20. Special Measures for Non-Cooperative Countries or Territories

20.1 The CBB requires UGB to give special attention to any dealings that it might have with corporates or persons domiciled in countries or territories which are:

- Identified by the FATF as being non cooperative countries or territories (NCCT)
- Notified to banks incorporated in Bahrain, by the CBB.[164]

20.2 The following is the list of NCCT and high risk countries, as identified by the FATF on the latest date of 24 October 2025.

Jurisdictions subject to a high risk and deemed non-cooperative with a call for action.[165]

Iran
Democratic People's Republic of Korea (DPRK)
Myanmar

Jurisdictions under Increased Monitoring

Algeria
Angola
Bolivia (newly added)
Bulgaria
Cameroon
Cote d'Ivoire
Democratic Republic of Congo
Haiti
Kenya
- Lao People's Democratic Republic (newly added)

Lebanon
Monaco
Namibia
Nepal

South Sudan
Syria
Venezuela
Vietnam
Virgin Islands – (UK)
Yemen

Source: https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html

20.3 In accordance with SWIFT's request and to limit any vulnerability of financial crime, no transactions should be undertaken where either the remitter or the beneficiary is domiciled in any of the above jurisdictions, or countries that are notified to Banks by the

164 FC 8.1.1

165 As per FATF List of October 2024

CBB.[166] Any exceptions (e.g. permitted transactions related to the UN) should be cleared by UGB's Compliance Department prior to processing the transactions. Similarly, if any inward remittances are received for individuals/ entities incorporated in this list, the MLRO/Deputy MLRO should be notified of the transaction/s within two days of receiving the remittance. Enhanced due diligence measures documenting the business relationship, the nature of the transaction and the purpose of the transaction, should be done by the MLRO/Deputy MLRO. The exception to this are the inward and outward remittances conducted on behalf of SPVs for which UGB is the legal owner that are domiciled in the Cayman Islands and/or British Virgin islands.

20.4 Money market or foreign exchange transactions conducted with banks for whom UGB has interbank limits, are excluded from the above category.

20.5 Operations will use the LSEG World Check screening tool and run a name-check against the beneficiary / remitter. A copy of the results from the will be printed and attached as an audit trail for clearance. All potential matches should be resolved by the MLRO/DMLRO.

20.6 Whenever transactions with parties domiciled in the NCCT list have no apparent economic or visible lawful purpose, their background and purpose must be examined and the findings documented. If suspicions remain about the transaction, these will be reported by the MLRO to the FID and the CBB. [167]

166 FC 8.1.1

167 FC 8.1.3

21. Other Requirements

21.1 Substantial Shareholdings Reporting - UGH

21.1.1 Any Person whose ownership alone or his ownership together with that of his minor children, or any other accounts under his disposal, or the ownership of any of his associate or affiliate companies amounts to 5% or more of any listed Security of a joint stock company on the Bahrain Bourse, will notify the licensed exchange forthwith, which shall in turn notify the CBB. The CBB may choose to make public, the name of the Person who owns such stake[168]

21.1.2 All persons whose ownership alone or whose ownership together with that of their minor children, or the accounts standing under their disposal amounts to 5% or more of any listed security in Bahrain, must conclude all transactions on such security on the Bahrain Bourse only. [169]

21.1.3. All persons must obtain CBB prior written approval to execute any order that will bring their ownership alone or their ownership together with their minor children, or the accounts standing under their disposal to 10% or more in any listed security. Any further increase of 1% or more shall also be subject to CBB prior written approval. [170]

21.1.4 It shall be prohibited to execute any purchase order issued by any client whose ownership alone or his ownership together with that of his minor children, or the accounts standing under his disposal amounts to 5% or more of any listed Security, and who wishes to carry out any transaction whether for his own account or any account standing under his disposal in a number of Securities representing 1% or more of such issue, unless such transaction is concluded on the Bahrain Bourse, and the CBB's prior written consent is obtained. [171] Any breach of this rule will result in the cancellation of the transaction. [172]

21.1.5 It shall be prohibited to execute any order issued by a client whose ownership amounts to 5% or more in any listed Security, and who wishes to own a stake of 10% or more of the company's shares, save upon ensuring that he has obtained written approval from the CBB to this effect.

21.2 Requirements for Deposit

A Security shall not be accepted in the Central Depository System unless its authenticity is approved by the concerned shares registrar and the client shall provide the Central Depository System with any amendment or change which may occur in such particulars.[173]

168 AML-7.1.1

169 AML-7.1.2

170 AML-7.1.2

171 AML-7.1.3

172 AML-7.1.4

173 AML-7.4.1

21.3 Acceptance of Cash by SRO Members

No cash transactions are permitted for customers.

22. Sanctions Compliance

UGB is committed to comply with ensuring that no individual or entity that is on defined global sanction lists issued by the OFAC, EU, CBB or CBK sanctions program is onboarded as a customer. It is hence mandatory for the Operations Team to screen the names of all potential customers against these applicable lists using the LSEG Worldcheck Tool. Once onboarded, the Worldcheck toggle should be set to 'Ongoing Screening', so that controls are in place to notify users or any alerts or red flags generated on customers. If there are any alerts, these should be escalated to the MLRO for resolution or for denying the onboarding of the customer.

A copy of the Worldcheck screening should be saved under the customer's folder in the UGB Customer Database at the time on-boarding, the annual MLRO reviews, customer KYC re-certification, change in the risk of the customer profile and on an ad-hoc basis (e.g. External Audit or Assurance reviews).

Sanctions Freezing Requirements: In the event UGB identifies a customer who is resident / incorporated in a sanctioned county or becomes a sanctioned country, it must :

- comply with the freezing requirements of the local regulator/ international body
- refrain from dealing with the customer and impose a freeze on the account
- notify the CBB through the Monthly Report on Exposure to Sanctioned Countries that is submitted by Accounts & Finance by the 10^{th} of each month.

23 Terrorist Financing

22.1 UNSCR

22.1.1 The Bank will comply in full of the provisions of the UN Security Council Anti-Terrorism Resolution No. 1373 of 2001 ("UNSCR 1373"). [174] This involves freezing without delay:

- funds and other financial assets or economic resources of persons who commit, or attempt to commit, terrorist acts or participate.
- in or facilitate the commission of terrorist acts; of entities owned or controlled.
- directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds derived or
- generated from property owned or controlled directly or indirectly by such persons
- and associated persons and entities.

174 FC-8.2.1

22.1.2 If UGB wishes, intends or has been requested to do anything that might contravene, in its reasonable opinion, the provisions of UNSCR 1373 , it will seek in writing the prior written opinion of the CBB on the matter.

22.1.3 The Bank will report to the CBB details of:

(a) Funds or other financial assets or economic resources held with them which may be fall under the scope of UNSCR 1373; and
(b) All claims, whether actual or contingent, which the Bank has on Persons and entities. All reports or notifications under this section will be made to the CBB's Compliance Directorate. [175]

A copy of the entire UNSCR 1373 resolution is included in Part B of Volume 1 of the CBB rulebook
http://cbb.complinet.com/cbb/display/display.html?rbid=1820&element_id=4139

Responses to the CBB or the Ministry of Interior affirming that the bank does not hold any account for individuals / entities named by either of them in circulars received by the Bank, should be sent within 5 days . The response should be sent by the MLRO/ Deputy MLRO in the pre-specified format found in Appendix 7 to the following email addresses:
cbb.circular.fid@cbb.gov.bh or
accfid@moiaffairs.gov.bh

Thel emails should be sent with the following text:
"With reference (Circular#) , kindly note that the listed individual/entity does not maintain an account with our institution (Bank Code: #30. UNIT) as per our records.[176]

Please find attached the required documents."

22.2 Designated Persons & Entities

22.2.1 The CBB from time-to-time issues to the Bank lists of designated Persons and entities believed to be linked to terrorism. UGB's MLRO is required to verify that the Bank has no dealings with these designated Persons and entities, and affirm the same to the CBB. Reporting will be done, using the forms provided by the CBB. [177]The CBB has to be notified of any funds or financial assets or economic resources, that contravene UNSCR 1373.

175 FC-8.2.6

176 As per the CBB's email dated 25 December2025 - Standardized Template for FI Responses to Circulars

177 FC-8.3.2, FC-8.2.4, FC-8,.2.6

22.2.2 Like other financial institutions incorporated in Bahrain, UGB is prohibited from dealing with any persons or entities designated by the CBB as potentially linked to terrorist activity. [178]

22.3 Predicate Crimes

A predicate crime is defined as an offense which is a component of a larger crime. Crimes that are specific to anti-money laundering programs have been referred to as Predicate Offenses UGB considers the proceeds of the following crimes to be predicate offences related to money laundering. If the Bank has suspicions or is aware that the monies in the account were sourced from one of the following predicate offenses, the Bank has the right refuse opening the account. If money is received from any of the following sources for an existing account, the Bank will immediately file a suspicious transaction.

Offense	FATF
Arms Trafficking	✓
Concealment of Assets	✓
Corruption & Bribery	✓
Counterfeiting Currency	✓
Counterfeiting Products	✓
Drug Trafficking	✓
Environmental Crime	✓
Extortion	✓
Forgery	✓
Fraud	✓
Human Trafficking / Migrant Smuggling	✓
Insider Trading & Market Manipulation	✓
Kidnapping, Illegal Restraint, and Hostage-taking	✓
Organized Crime / Racketeering	✓
Piracy	✓
Robbery or Theft	✓
Sexual Exploitation	✓

178 FC-8.3.1

Smuggling	✓
Tax Crimes	✓
Terrorism / Terrorist Financing	✓
Trafficking in Stolen Goods	✓
Violent Crime (Murder & Grievous Bodily Injury)	✓

23. Regulatory Penalties

23.1 Financial penalties for failure to comply with CBB rules on AML

Without prejudice to any other penalty imposed by the CBB Law, the AML Law No. 4 or the Penal Code of the Kingdom of Bahrain

- Failure by a Bank to comply with the CBB rules or any directive, shall result in the levying by the CBB, without need of a court order and at the CBB's discretion, of a fine of up to BD 20,000.

- Any person convicted of committing, attempting of participating in a money laundering offence: (Article 3.1)
  - Prison up to 7 years, and
  - BD 1,000,000 maximum fine

- The punishment shall be imprisonment for a period of not less than five (5) years and fine of not less than Bahrain Dinars One Hundred Thousand (BD 100,000/-) in any of the following cases:
  - the accused has committed the offence through an organised criminal gang;
  - the accused has committed the offence by using his power or influence through an institution;
  - the accused has committed the offence for the purpose of disguising the source of the proceeds which are derived from criminal activity to appear as of a lawful source.

23.2 Financial penalties for late submission of AML related reports

Delays after 30th June for each financial year, for submitting the external auditor's assurance report on the AML CFT Controls within UGB and its subsidiaries, can result in a penalty of BD 200 per day,

Appendices

Appendix 1 – Examples of suspicious transactions

1. Transactions using Customers' Accounts:

1.1 Customers who maintain a number of trustee or customers' accounts are not required by the type of business they conduct, particularly if there were transactions which contain names of unknown persons.

1.2 Customers who have numerous accounts and pay in amounts of cash to each of these accounts, whereby the total of credits is a large amount except, for institutions which maintain these accounts for Banking relationships with Banks which extend to them facilities from time to time.

1.3 Any individual or company whose account shows no normal personal Banking or business-related activities, but is used to receive or disburse large sums which have no obvious purpose or for a purpose not related to the account holder and/or his business (e.g., a substantial turn-over in the account).

1.4 Any individual or company whose account shows virtually no normal personal Banking or business-related activities, but is used to receive or disburse large sums which have no obvious purpose or for a purpose not related to the account holder and/or his business (e.g., substantial turn-over in the account).

1.5 Customers who have accounts with several financial institutions within the same locality and who transfer the balances of those accounts to one account, then transfer the consolidated amount to a person abroad.

1.6 Paying-in large third-party cheques endorsed in favor of the account holder when they do not seem to be relevant to the account holder and his nature of business.

1.7 Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received unexpectedly large sums of money from abroad.

1.8 A large number of individuals deposit monies into the same account without an adequate explanation.

1.9 Unusually large deposits in the accounts of a jewelry shop whose accounts have never witnessed such deposits particularly, if a large part of these deposits is in cash.

2. Suspicious Investment-related Transactions:

2.1 Purchasing of securities to be held by the financial institution in safe custody, where this does not appear appropriate given the customer's apparent standing.

2.2 Individual or commercial institutions bring in large sums of money to invest in foreign currencies or securities, where the size of transactions is not consistent with the income of the concerned individual or commercial institutions.

2.3 Buying or selling of securities with no justifiable purpose or in circumstances which appear unusual.

3. Suspicious International Banking and Financial Transactions:

3.1 Customers introduced by a branch outside the country, an affiliate, or another Bank, based in one of the countries known for the production or consumption of drugs or other serious criminal activities.

3.2 Building up of large balances not consistent with the known turnover of the customer's business, and the subsequent transfer to account(s) held abroad.

3.3 Frequent requests for travelers' cheques, foreign currency drafts or other negotiable instruments, for no obvious reasons.

3.4 Frequent paying-in of travelers' cheques or foreign currency drafts large amounts for no obvious reasons, particularly if originating from abroad.

4. Suspicious use of Letters of Credit:

4.1 Where the Bank's customer who opens these letters is the beneficiary and the owner of the shipping company.

4.2 Where amounts on letters of credit submitted by the customer to the Bank and to the Customs/Port/Airport authorities do not match the original.

4.3 Where the size of the facilities is not in line with the securities on hand, nature of business and net-worth of the customers.

4.4 Where such trade is not consistent with the customer's usual business.

5. Suspicious Loan Transactions:

5.1 Customers who repay classified/problem loans before the expected time and for larger amounts than anticipated.

5.2 Customers who request loans against assets held by the financial institutions or third party, where the origin of those assets is not known, or the assets are inconsistent with the customer's standing.

5.3 Non-resident individuals who request loans secured by Bank guarantees issued by foreign Banks where the purpose of the transaction is questionable.

5.4. Loan transactions against pledge of deposits with financial institutions outside the country, especially if these were in countries known for the production, processing, or consumption of drugs or other serious criminal activities.

6. Suspicious Transactions using Electronic Banking Services:

6.1 When an account receives numerous small fund transfers electronically, and then the account holder carries out large transfers in the same way to another country.

6.2. Where a customer makes regular and large payments using different means including electronic payments that cannot be clearly identified as Bonafide transactions, or receive regular and large payments from countries known for serious criminal activities.

6.3. Where transfers from abroad, which are received in the name of a customer of the Bank or any financial institution electronically, are then transferred abroad in the same way without passing through an account (i.e., they are not deposited then withdrawn from the account). Such transactions should be registered in the account and should appear in the account statement.

7. Suspicious Cash Transactions

7.1 Unusually large cash deposits made by an individual or a company whose normal business activity would mainly by conducted by Cheques or other instruments.

7.2 Substantial increase in cash deposits by any customer or Financial Institution without an apparent cause, especially if such deposits are subsequently transferred within a short period out of the account to a destination not normally associated with the customers.

7.3 Customers who deposit cash in numerous stages so that the amount of each deposit it below BD 6,000, but the total of which is equal to or exceeds that amount.

7.4 Company accounts whose transactions, both deposits and withdrawals, are conducted in cash rather than in negotiable instruments (e.g., Cheques, letters of credit, drafts etc.) without an apparent reason.

7.5 Customers who constantly pay-in or deposit cash to cover requests for bankers' drafts, money transfers or other negotiable instruments without an apparent reason.

7.6 Customers who seek to change large quantities of lower denomination banknotes for those of higher denomination banknotes with no obvious reasons.

7.7 Customers who transfer large sums of money outside the country with instructions for payment in cash, and large sums transferred from outside the country in favor of non-resident customers with instructions for payment in cash.

7.8 Unusually large cash deposits using “ATMS” or “cash deposit machine” to avoid direct contact with the employees of the relevant licensee, if such deposits are not consistent with the business/normal income of the concerned customers.

Appendix 2 – Annual AML Questionnaire from UGB's financial subsidiaries

Date:

Name of the subsidiary
Country of incorporation
Countries where the subsidiary operates.

#	**Item**	**Comments**
1	When was the last AML Policy approved by the Board of Directors?	
2	When was the MLRO's Annual AML report containing the assessment of AML controls and customer due diligence submitted to the Board of Directors?	
3	When was the last HR policy approved which includes adequate screening procedures and controls taken while hiring employees?	
4	When was the last AML training conducted for your institution?	
	How many staff attended the above AML training? (Number and %)	
	When were members of the Board of Directors last trained in AML ?	
	How many Directors have been provided the above AML training? (Number and %)	
5	When was the last audit of the AML function conducted by your internal audit department?	
	How many audit points are still open as of the date of this response?	
	What are the open points and the proposed date for the closure of the above points?	
6	When was the last audit of the AML function conducted by your external auditor / regulator?	
	How many audit points are still open as of the date of this response?	
	What are the open points and the proposed date for the closure of the above points?	

7	What policies and procedures do you have for sharing information internally and externally with your financial regulator for the purposes of CDD and money laundering and terrorist financing risk management.	
	When was this last approved?	
8	What policy do you have to ensure that there are adequate safeguards on the confidentiality and use of information exchanged?	
	When was this last approved by the Board of Directors?	
9	Do you have any subsidiaries which are financial institutions to which AML/CFT standards apply?	
	If the answer to the above is yes, please explain what controls you have in place to ensure that the subsidiaries adhere to the AML/CFT standards?	

Name of the MLRO

Signature

Appendix 3 – Template of MLRO Review - Entity

Name of Customer	
Account #	
Date of Opening of Account	
Country of tax residency	
Risk Category (at the time of onboarding)	

Dimension		Rating
Customer		
Country		
Products/ Services		
Channel of Communication		
Current Risk Rating (as per AML risk matrix)		

Source of Funds as per KYC

Status of Documentation

Account Opening Form	
Articles of Association	
Beneficial Ownership Chart	
Board Resolution	
Commercial Registration	
FATCA / CRS Form	
Fax and email Indemnity	
KYC	
Passport Copies	
Signature Card	
W8 BEN / W8 BEN E/ W9	
Worldcheck Review Date	

Account Behavior During the Year

Anticipated Value of Transactions (from the KYC form)	
Actual Value of Transactions	
Number and nature of any significant transactions	
Changes in the way that the bank account is operated or in the manner in which the business relationship is conducted	
Patterns and behavior	
Risk Profile at the time of onboarding	
Current Risk Profile	

Additional Observations if any by the MLRO

Appendix 4 – Template of MLRO Review – Individual

Name of Customer	
Account #	
Date of Opening of Account	
Country of Tax Residency	
Risk Category at the time of on-boarding	

Dimension	**Description**	**Rating**
Customer		
Country		
Products/ Services		
Channel of Communication		
Risk Category		

Source of Funds as per KYC

Status of Documentation

Account Opening Form	
Articles of Association	
Beneficial Ownership Chart	
Board Resolution	
Commercial Registration	
FATCA / CRS Form	
Fax and email Indemnity	
KYC	
Passport Copies	
Signature Card	
W8 BEN / W8 BEN E/ W9	
Worldcheck Review Date	

Account Behavior During the Year

Anticipated Value of Transactions (from the KYC form)	
Actual Value of Transactions	
Number and nature of any significant transactions	
Changes in the way that the bank account is operated or in the manner in which the business relationship is conducted	
Patterns and behavior	

Risk Profile at the time of onboarding	
Current Risk Profile	

Additional Observations if any by the MLRO –

Appendix 5 – Geographical Risk Score and List of Prohibited Countries as per Burgan Bank KPSC

Ref.	Country Name	Group AFC Q4 - Siron Risk Score	Group AFC Q4 - CRAM Risk Score
1	Afghanistan, Islamic Republic of	High	High
2	Åland Islands	Low	Low
3	Albania, Republic of	Medium	Medium
4	Algeria, People's Democratic Republic of (El Djazaïr)	Medium	Medium
5	American Samoa	Medium	Medium
6	Andorra, Principality of	Low	Low
7	Angola, Republic of	High	High
8	Anguilla (Overseas Territory of the United Kingdom)	Medium	Medium
9	Antarctica	Low	Low
10	Antigua and Barbuda	Medium	Medium
11	Argentina, Republica	Medium	Medium
12	Armenia, Republic of	Medium	Medium
13	Aruba (Kingdom of the Netherlands)	Medium	Medium
14	Australia, Commonwealth of	Low	Low
15	Austria, Republic of	Low	Low
16	Azerbaijan, Republic of	Medium	Medium
17	Bahamas, Commonwealth of the	Medium	Medium
18	Bahrain, Kingdom of	Medium	Medium
19	Bangladesh, People's Republic of	Medium	Medium
20	Barbados	Medium	Medium
21	Bedoun ***	Medium	Medium
22	Belarus, Republic of	Prohibited	Very High
23	Belgium, Kingdom of	Low	Low
24	Belize	Medium	Medium
25	Benin, Republic of	Medium	Medium
26	Bermuda Islands, the	Low	Low
27	Bhutan, Kingdom of	Low	Low
28	Bolivia, Republic of (Plurinational State)	High	High
29	Bonaire, Sint Eustatius and Saba	Low	Low
30	Bosnia and Herzegovina	Medium	Medium
31	Botswana, Republic of	Low	Low
32	Bouvet Island	Low	Low
33	Brazil, Federative Republic of	Medium	Medium
34	British Indian Ocean Territory	Medium	Medium
35	British Virgin Islands (Overseas Territory of the United Kingdom)	High	High
36	Brunei Darussalam, Negara	Medium	Medium
37	Bulgaria, Republic of	Medium	Medium

38	Burkina Faso	**High**	**High**
39	Burundi, Republic of	**Medium**	**Medium**
40	Cambodia, Kingdom of	**Medium**	**Medium**
41	Cameroon, Republic of	**High**	**High**
42	Canada	**Low**	**Low**
43	Cape Verde, Republic of	**Medium**	**Medium**
44	Cayman Islands	**Medium**	**Medium**
45	Central African Republic	**High**	**High**
46	Chad, Republic of (tchad)	**Medium**	**Medium**
47	Chile, Republic of	**Low**	**Low**
48	China, People's Republic of	**Medium**	**Medium**
49	Christmas Island, Territory of	**Low**	**Low**
50	Cocos (Keeling) Islands, Territory of	**Low**	**Low**
51	Colombia, Republic of	**Medium**	**Medium**
52	Comoros, Union of the	**Medium**	**Medium**
53	Congo, Democratic Republic of the (formerly Zaire)	**High**	**High**
54	Congo, Republic of	**Medium**	**Medium**
55	Cook Islands	**Medium**	**Medium**
56	Costa Rica, Republic of	**Medium**	**Medium**
57	Côte d'Ivoire, Republic of (Ivory Coast)	**Medium**	**Medium**
58	Croatia, Republic of (Hrvatska)	**Medium**	**Medium**
59	Cuba, Republic of	**Prohibited**	**Very High**
60	Curaçao	**Medium**	**Medium**
61	Cyprus, Republic of	**Medium**	**Medium**
62	Czech Republic	**Low**	**Low**
63	Denmark, Kingdom of	**Low**	**Low**
64	Djibouti, Republic of	**Medium**	**Medium**
65	Dominica, Commonwealth of	**Medium**	**Medium**
66	Dominican Republic	**Medium**	**Medium**
67	Ecuador, Republic of	**Medium**	**Medium**
68	Egypt, Arab Republic of	**Medium**	**Medium**
69	El Salvador, Republic of	**Medium**	**Medium**
70	Equatorial Guinea, Republic of	**Medium**	**Medium**
71	Eritrea, State of	**High**	**High**
72	Estonia, Republic of	**Low**	**Low**
73	Ethiopia, Federal Democratic Republic of	**Medium**	**Medium**
74	Falkland Islands (Islas Malvinas)	**Low**	**Low**
75	Faroe Islands	**Low**	**Low**
76	Fiji Islands, Republic of the	**Medium**	**Medium**
77	Finland, Republic of	**Low**	**Low**
78	France (French Republic)	**Low**	**Low**
79	French Guiana (Région Guyane)	**Low**	**Low**
80	French Polynesia	**Low**	**Low**

81	French Southern and Antarctic Lands, Territory of the	**Low**	**Low**
82	Fürstentum Liechtenstein	**Low**	**Low**
83	Gabon (Gabonese Republic)	**Medium**	**Medium**
84	Gambia, Republic of the	**Medium**	**Medium**
85	Georgia (Sakartvelo)	**Medium**	**Medium**
86	Germany (Deutschland)	**Low**	**Low**
87	Ghana, Republic	**Medium**	**Medium**
88	Gibraltar (Overseas Territory of the United Kingdom)	**Medium**	**Medium**
89	Greece (Hellenic Republic)	**Low**	**Low**
90	Greenland	**Low**	**Low**
91	Grenada	**Medium**	**Medium**
92	Guadeloupe (Région Guadeloupe)	**Low**	**Low**
93	Guam, Territory of	**Medium**	**Medium**
94	Guatemala, Republic of	**Medium**	**Medium**
95	Guernsey, Bailiwick of (Channel Islands, Crown Dep of the UK)	**Medium**	**Medium**
96	Guinea, Republic of {Guinea Conakry}	**Medium**	**Medium**
97	Guinea-Bissau, Republic of	**Medium**	**Medium**
98	Guyana, Co-operative Republic of	**Medium**	**Medium**
99	Haiti, Republic of	**High**	**High**
100	Heard Island and McDonald Islands	**Low**	**Low**
101	Honduras, Republic of	**Medium**	**Medium**
102	Hong Kong (Special Administrative Region)	**Medium**	**Medium**
103	Hungary, Republic of	**Medium**	**Medium**
104	Iceland, Republic of	**Low**	**Low**
105	India, Republic of	**Medium**	**Medium**
106	Indonesia, Republic of	**Medium**	**Medium**
107	Iran, Islamic Republic of	**Prohibited**	**Very High**
108	Iraq, Republic of	**High**	**High**
109	Ireland (Eire)	**Low**	**Low**
110	Isle of Man (Crown Dependency of the United Kingdom)	**Low**	**Low**
111	Israel, State of	**Prohibited**	**Prohibited**
112	Italy (Italian Republic)	**Low**	**Low**
113	Jamaica	**Medium**	**Medium**
114	Japan (Nippon-koku)	**Low**	**Low**
115	Jersey, Bailiwick of (Channel Islands, Crown Dep of the UK)	**Low**	**Low**
116	Jordan, Hashemite Kingdom of	**Medium**	**Medium**
117	Kazakhstan, Republic of	**Medium**	**Medium**
118	Kenya, Republic of	**High**	**High**
119	Kiribati, Republic of	**Medium**	**Medium**
120	Korea, Democratic People's Republic of [North]	**Prohibited**	**Prohibited**

121	Korea, Republic of [South]	Low	Low
122	Kosovo, Republic Of {partially recognized}	Medium	Medium
123	Kuwait, State of ***	Medium	Medium
124	Kyrgyzstan (Kyrgyz Republic)	Medium	Medium
125	Lao, People's Democratic Republic	High	High
126	Latvia, Republic of	Low	Low
127	Lebanese Republic	High	High
128	Lesotho, Kingdom of	Medium	Medium
129	Liberia, Republic of	Medium	Medium
130	Libyan Arab Jamahiriya, Great Socialist People's	High	High
131	Lithuania, Republic of	Low	Low
132	Luxembourg, Grand Duchy of	Low	Low
133	Macau (Special Administrative Region)	Medium	Medium
134	Macedonia, Republic of (Former Yugoslav …)	Medium	Medium
135	Madagascar, Republic of	Medium	Medium
136	Malawi, Republic of	Medium	Medium
137	Malaysia	Medium	Medium
138	Maldives, Republic of	Medium	Medium
139	Mali, Republic of	High	High
140	Malta, Republic of	Low	Low
141	Marshall Islands, Republic of	Medium	Medium
142	Martinique (Région Martinique)	Low	Low
143	Mauritania, Islamic Republic of	Medium	Medium
144	Mauritius, Republic of	Low	Low
145	Mayotte, Collectivité départementale de	Low	Low
146	México (United Mexican States)	Medium	Medium
147	Micronesia, Federated States of	Medium	Medium
148	Moldova, Republic of	Medium	Medium
149	Monaco, Principality of	Medium	Medium
150	Mongolia	Medium	Medium
151	Montenegro	Medium	Medium
152	Montserrat	Medium	Medium
153	Morocco, Kingdom of	Medium	Medium
154	Mozambique, Republic of	Medium	Medium
155	Myanmar, Union of (formerly Burma)	Prohibited	High
156	Namibia, Republic of	Medium	Medium
157	Nauru, Republic of	Medium	Medium
158	Nepal, Federal Democratic Republic of	Medium	Medium
159	Netherlands, Kingdom of the	Low	Low
160	New Caledonia	Low	Low
161	New Zealand	Low	Low
162	Nicaragua, Republic of	Medium	Medium
163	Niger, Republic of	Medium	Medium

164	Nigeria, Federal Republic of	High	High
165	Niuē Fekai	Medium	Medium
166	Norfolk Island, Territory of	Low	Low
167	Northern Marina Islands, Commonwealth of the	Low	Low
168	Norway, Kingdom of	Low	Low
169	Oman, Sultanate of	Low	Low
170	Pakistan, Islamic Republic of	Medium	Medium
171	Palau, Republic of	Medium	Medium
172	Palestinian Territory, Occupied (incl West Bank/Gaza Strip)	High	High
173	Panama, Republic of	Medium	Medium
174	Papua New Guinea, Independent State of	Medium	Medium
175	Paraguay, Republic of	Medium	Medium
176	Perú, Republic of	Medium	Medium
177	Philippines, Republic of the	Medium	Medium
178	Pitcairn Islands	Medium	Medium
179	Poland, Republic of	Low	Low
180	Portugal (Portuguese Republic)	Low	Low
181	Puerto Rico, Commonwealth of	Medium	Medium
182	Qatar, State of	Medium	Medium
183	Réunion (Région Réunion)	Low	Low
184	Romania	Medium	Medium
185	Russian Federation	Prohibited	Very High
186	Rwanda, Republic of	Medium	Medium
187	Saint Barthélemy, Collectivity of	Low	Low
188	Saint Helena and Ascension and Tristan da Cunha	Medium	Medium
189	Saint Kitts and Nevis, Federation of	Medium	Medium
190	Saint Lucia	Medium	Medium
191	Saint Martin, Collectivity of (French Part)	Medium	Medium
192	Saint Pierre And Miquelon, Territorial Collectivity of	Low	Low
193	Saint Vincent and the Grenadines	Medium	Medium
194	Samoa, Independent State of (formerly Western Samoa)	Medium	Medium
195	San Marino, Most Serene Republic of	Low	Low
196	São Tomé and Principe, Democratic Republic of	Medium	Medium
197	Saudi Arabia, Kingdom of	Medium	Medium
198	Senegal, Republic of	Medium	Medium
199	Serbia, Republic of	Medium	Medium
200	Seychelles, Republic of	Medium	Medium
201	Sierra Leone, Republic of	Medium	Medium
202	Singapore, Republic of	Low	Low
203	Sint Maarten (Dutch Part)	Medium	Medium
204	Slovakia (Slovak Republic)	Low	Low
205	Slovenia, Republic of	Medium	Medium

206	Solomon Islands	**Medium**	**Medium**
207	Somalia (Somali Republic)	**High**	**High**
208	South Africa, Republic of (Zuid Afrika)	**Medium**	**Medium**
209	South Georgia and the South Sandwich Islands	**Low**	**Low**
210	South Sudan, Republic Of	**Prohibited**	**Very High**
211	Spain, Kingdom of (España)	**Low**	**Low**
212	Sri Lanka, Democratic Socialist Republic of (formerly Ceylon)	**Medium**	**Medium**
213	Sudan, Republic of	**Prohibited**	**Very High**
214	Suriname, Republic of	**Medium**	**Medium**
215	Svalbard and Jan Mayen	**Low**	**Low**
216	Swaziland, Kingdom of (aka Eswatini)	**Medium**	**Medium**
217	Sweden, Kingdom of	**Low**	**Low**
218	Switzerland (Swiss Confederation)	**Low**	**Low**
219	Syrian Arab Republic (Syria)	**High**	**High**
220	Taiwan	**Medium**	**Medium**
221	Tajikistan, Republic of	**Medium**	**Medium**
222	Tanzania, United Republic of	**Medium**	**Medium**
223	Thailand, Kingdom of	**Medium**	**Medium**
224	Timor-Leste, Democratic Republic of (formerly East Timor)	**Medium**	**Medium**
225	Togo (Togolese Republic)	**Medium**	**Medium**
226	Tokelau	**Low**	**Low**
227	Tonga, Kingdom of	**Medium**	**Medium**
228	Trinidad and Tobago, Republic of	**Medium**	**Medium**
229	Tunisia (Tunisian Republic)	**Medium**	**Medium**
230	Turkey, Republic of	**Medium**	**Medium**
231	Turkmenistan	**Medium**	**Medium**
232	Turks and Caicos Islands	**Medium**	**Medium**
233	Tuvalu (formerly Ellice Islands)	**Medium**	**Medium**
234	U.S. Virgin Islands	**Medium**	**Medium**
235	Uganda, Republic of	**Medium**	**Medium**
236	Ukraine	**Medium**	**Medium**
237	United Arab Emirates	**Medium**	**Medium**
238	United Kingdom of Great Britain and Northern Ireland	**Low**	**Low**
239	United States Minor Outlying Islands	**Low**	**Low**
240	United States of America	**Low**	**Low**
241	Uruguay, Eastern Republic of	**Low**	**Low**
242	Uzbekistan, Republic of	**Medium**	**Medium**
243	Vanuatu, Republic of	**Medium**	**Medium**
244	Vatican City, State of the (Holy See)	**Medium**	**Medium**
245	Venezuela, Bolivarian Republic of	**High**	**High**
246	Vietnam, Socialist Republic of	**High**	**High**

247	Wallis and Futuna Islands, Territory of	**Low**	**Low**
248	Western Sahara (formerly Spanish Sahara)	**Medium**	**Medium**
249	Yemen, Republic of	**Prohibited**	**High**
250	Zambia, Republic of (formerly Northern Rhodesia)	**Low**	**Low**
251	Zimbabwe, Republic of (formerly Southern Rhodesia)	**Medium**	**Medium**
252	Treat As Kuwaiti	**Medium**	**Medium**

Appendix 6 – Template of Risk Scoring – Individuals & Entities

Client Name
Customer Account Number
Date of Review

AML Risk Assessment Matrix

#	Customer AML Risk Factor	Yes	No	Risk Score
A	**Customer Profile**			
1	Individual / Entity is a non-resident	x		3
2	Individuals / Entities has a net worth of < 1 million			0
3	Individuals / Entities has a net worth of > 1 Million	x		3
4	Individuals/ Entities are categorized as politically exposed persons (PEPs)	x		3
5	Individuals/Entities have been sanctioned by the UN, EU, OFAC or any other regulatory body.			0
6	STRs have been filed by UGB on the activity of the individual/entity.			0
7	Individuals/Entities have a negative history in World check / public sources.			0
8	Individuals / entities establish a relationship with UGB under unusual circumstances (e.g. significant unexplained geographic distance between the financial institution and the customer).			0

9	Individuals/Entities have arrangements to be personal asset-holding vehicles or operate the account on behalf of a third party.			0
10	Individuals/Entities have nominee shareholders or shares in bearer form.			0
11	Entities have a non-transparent ownership structure.			0
12	The ownership structure of the entity appears unusual or excessively complex given the nature of the entity's business.			0
13	Individual / entity is engaged in, or derives wealth or revenues from, a high-risk cash-intensive businesses or high risk jurisdictions			0
14	UBO information is unavailable			0
	Total			9
	Customer Risk Score		**60%**	**5.4**
B	**Country /Geography**			
1	Customer is resident / incorporated in OECD country			0
2	Customer is resident / incorporated in GCC country	x		2
3	Customer is resident / incorporated in FATF designated NCCT country or FATF/EU designated country with strategic deficiencies/ non-cooperative jurisdictions for tax purposes			0

4	Customer is resident / incorporated in countries subject to war / civil unrest/ significant corruption/ organized crime/criminal activity.			0
5	Customer is resident / incorporated in countries subject to sanctions			0
6	Customer is resident / incorporated in countries identified as having weak governance, law enforcement and regulatory regimes			0
7	Customer is resident / incorporated in countries with banking secrecy laws that prohibit release of beneficial ownership information			0
	Total			1
	Geography Risk Score		**20%**	**0.4**
C	**Products/Services/Transaction Risk**			
1	Assets under custody			0
2	Brokerage			0
3	Deposits	x		2
4	Investments	x		2
5	Loans			0
6	Trade Finance			0
	Total		**10**	4
	Product Risk Score		10%	**0.4**

D	**Channel of Distribution**			
1	Customer provides Face to face instructions			0
2	Customer provides SWIFT based or Authenticated Test Code instructions			0
3	Pattern of wire transfer activity shows unusual patterns or has no apparent purpose.			0
4	Customer provides Unauthenticated instructions or non SWIFT instructions that are provided only on mail, e-mail, phone, fax	x		3
5	Customer's Non-face-to-face instructions are received from Gatekeepers. These could include intermediaries suspected of criminal activities, located in a country with a weak AML/CFT regime, history of non compliance with laws or regulations, or weak governance.			0
	Total			3
	Channel of Distribution Risk Score		5%	**0.15**
E	**Terrorism and Proliferation Financing Risk Score**			
1	Customer's transactions involve person or entity in a foreign country of proliferation concern. (North Korea, Iran and Myanmar)			0
2	Customer's transactions involve shipment of goods incompatible with the technical level of the country to which it is being shipped, (e.g., semiconductor manufacturing equipment being shipped to a country that has no electronics industry).			0

3	Customer's transactions involve persons or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws.			0
4	Customer's transactions involve shipment of goods inconsistent with normal geographic trade patterns			0
5	Customer's transactions involve dual-used goods, proliferation sensitive or military goods.			0
6	Wire instructions or payment are made from or due to parties not identified on the original letter of credit or other documentation.			0
7	Description of goods on trade or financial documentation is non-specific, innocuous or misleading.			0
8	Information on the end-use or final destination of the trade finance transaction is unclear.			0
9	A freight forwarding firm is listed as the product's final destination.			0
10	Order for goods is placed by firms or persons from foreign countries other than the country of stated end-user.			0
	Total			0
	Proliferation Financing Risk Score		5%	
	Weighted Risk Score Calculation	**Weightage**	**Score**	**Score**
	Customer Risk Profile	60%	9	5.4
	Geographic Risk Profile	20%	1	0.2
	Product Risk Profile	10%	4	0.4
	Channel of distribution Risk Profile	5%	3	0.15
	Proliferation Financing Risk Profile	5%	0	0
	Core Score	100%	17	
	Weighted Risk Score Calculation			**6.35**

Due Diligence Level	Low Risk (1 - 3)	Medium Risk (3.01 - 6)	High Risk (6.01 - 7.5)	Significantly High Risk (>7.6)
	Normal Due Diligence		Enhanced Due Diligence	
			x	

Appendix 7 – Documentation Checklist:

☐ Account Opening Form including terms and conditions.

☐ Authorized Signatory List, UGB Signature Card & Certified photocopies of the passport and CPR/ Civil ID / Government issued national identification proof of signatories permitted to operate the UGB account.

☐ Bankers' / Group introduction certificate

☐ Board Resolution seeking banking services / opening of the account and authorizing the named signatories to operate the account.

☐ Commercial Registration or Certificate of Incorporation

☐ FATCA CRS self-certification forms

☐ Fax/ Email indemnity

☐ KYC Forms

☐ Latest audited financial statements

☐ Memorandum and Articles of Association

☐ Name of ultimate beneficial owner (UBO) * and his/her attested identification document

☐ Names, country of residence and nationality of Directors names of the relevant people having a senior management position in the legal entity.

☐ Ownership structure chart (all entities owning 10% or more of the issued capital)

☐ Proof of registered address (utility bill or bank statement; this should show a physical address - not only a PO Box)

☐ Power of attorney (if applicable)

☐ W8 BEN/ W8 BEN E / W9 forms

☐ Sanctions Exposure Questionnaire

And Written Approval from the CEO to open the account.

Appendix 8 – Format of response to be sent to the CBB or the Ministry of Interior

مصرف البحرين المركزي
Central Bank of Bahrain

Account Request Form

Anti-Financial Crime Directorate | Circular Reference no.

Please complete the following:

☐ **Yes, we maintain an account / transaction (Account statements required)**

☒ **No, we do not maintain an account / transaction.**

S. No.	Name	CPR / CR / PPN No.	Account No.	Account Type\Card limit	Opening Date	Closing Date	Status	Balance
1.								
2.								

Kindly return the duly completed form to the CBB Anti-Financial Crime Directorate by e-mail, not later than five working days from the date of this circular. The undersigned hereby takes the full responsibility to maintain the confidentiality of the above and to provide all the information required.

Bank's Name: United Gulf Bank B.S.C. (c) **Bank Code** UNIT **MLRO's Name:**______

Date: **Signature:**

Version Control

Version #	Date Issued	Originator/ Modified By	Reason for Issue / Re-Issue
1	April 2011	MLRO/OPS	• Updated to reflect current new CBB AML regulations.
2	August 2013	Compliance / MLRO	• Updated to reflect current new CBB AML regulations.
3	March 2015	Compliance / MLRO	• Updated to reflect current new CBB AML regulations.
4	April 2016	Compliance / MLRO	• Updated to reflect the requirement to get FATCA self-certifications and forms; current list of NCCT countries and record keeping tenor as specified by the Capital Markets Supervision Directorate
5	February 2017	Compliance/MLRO	• Updated List of NCCT countries
6.	January 2018	Compliance/MLRO	• Updated new rules relating to AML requirement of subsidiaries; references to the UGB Customer Data system; list of NCCT countries and inclusion of new forms for KYC and FATCA/CRS
7.	February 2019	Compliance/MLRO	• Updated List of NCCT countries
8.	June 2020	Compliance/MLRO	• Documenting the risk matrix on four dimensions of customer profile, geography, products and services and channels to determine the risk profile of the customer. • Developing a detailed set of AMLS related KPIs per department in order to incorporate in the yearly assessments. • Updated List of NCCT countries
9	February 2021	Compliance / MLRO	• Documenting the requirements of identifying the Ultimate Beneficial Owner • Restriction on money transfers to cryptocurrency exchanges and digital wallets.

			• Documenting the Bank's definition of predicate crimes to satisfy Wolfsberg requirements • Reference to Bahrain's Personal Data Protection Law No. 30 of 2018 and the need to protect personal, sensitive information. • Documenting the process of Annual MLRO reviews.
10	March 2022	Compliance / MLRO	• Introduction of the term Proliferation Financing as part of AML and CFT • Adoption of the risk based approach and the methodology for deriving the risk score for the purposes of customer profiling • Updated List of countries designated as high risk. • Emphasis on documentation of the UBO, the ownership structure and other official/government issued identification at the time of onboarding. This includes the Group Introduction Certificate / banker's assurance certificate. • Introduction of the Annual AML Questionnaire from UGB's financial subsidiaries • Revamped Appendix 12 - Money Laundering STR Internal Report Form • Revamped Appendix 13 - MLRO Suspicion Evaluation Record • Revamped Appendix 14 - External Suspicious Transaction Report Form
11	February 2023	28 February 2023	• Inclusion of a separate section on non-residents • Introduction of Appendix 11 – Group Introduction Letter. • Change in the process of reporting STRs externally to the Ministry of Interior's IIS system.

12	November 2023	13 November 2023	• Update incorporates areas of improvement / closure of gaps highlighted in the AML Enterprise Wide Risk Assessment exercise conducted by Keypoint WLL. The main changes are : • Adding a section on the annual screening of UGB's employees • Use of reports from Know Your Country.com to assist in determining Geography / Country Risk • Changes in the product risk dimension • Inclusion of a fifth dimension for risk scoring that is related to the PF/WMD risk for customers using trade finance products • Implementing a weighted average risk methodology across dimensions. • Updated bands for risk weights • Reinstating UGH's simplified risk scoring for financial counterparties. • Inclusion of quarterly AML monitoring in the BAC reports • New procedures governing AML review of new products / ventures. • Updating the countries on the FATF black and grey lists. • Introduction of a Sanctions Questionnaire for corporates
13	February 2024	28 February 2024	• Addition of place of birth as a field for customer due diligence (for an individual) • Addition of the requirement to notify customers of any services which may be restricted or otherwise limited, as a result of their non- resident status based on the results of the risk scoring and risk assessment.

			• Addition of the requirement for the Bank to report to the Compliance Directorate, all assets frozen or actions taken in compliance with the instructions of the CBB with respect to their circulars received with respect to United Nations Security Council Resolutions
14	February 2025	28 February 2025	• Updated List of jurisdictions under increased monitoring • Inclusion of a statement that UGB will not open accounts for companies under formation.
15	February 2026		• Expansion of the Scope of the PPM to cover UGB's responsibility as a Parent, responsibilities of UGB's subsidiaries and UGB's responsibilities to its parent Burgan Bank. • Introduction of Section 3.1 – list of prohibited industries. Customers operating in these industries will not be onboarded. • Addition of Section 6.2 - Independent verification of employment or public position held. If the account is opened for an employee of any of the Bank's subsidiaries or parent, a letter from the HR Department of the subsidiary confirming employment and the position, should be obtained. • Expansion of the definition of PEP in Section 6.3 to include other categories as specified by the Bank's parent Burgan Bank. • Expansion of Section 7 to include more information that needs to be maintained in the UGB Customer Database. • Expansion of Section 9.2 to include prohibited countries and transactions involving prohibited countries. It also involves a change in the Bank's methodology of assigning the geographical score of the customer. UGB will adopt the more conservative score between those published by Know Your Country.com and

			Burgan Bank's internal assessment of a country. • Expansion of Section 9.3. to assign a higher risk to non-face-to-face business relationships sourced through a professional intermediary. • Addition of Section 13.4 and Section 13.6 covering the MLRO's reporting to the BAC /Board and Burgan Bank's GAFC. • Addition of Section 13.7 to include AML controls and responsibilities conducted by other departments of UGB. • Expansion of Section 14.2 to cover the responsibilities of staff and the MLRO in compiling and maintaining documentation on internal STRs. • Expansion of Section 18.1 to make annual AML / Sanctions training mandatory for all independent directors and staff. Additional AML training will be provided to staff who score poorly on the annual Aml assessment. • Update of Section 20 to reflect the latest list of countries designated as high risk by the FATF. • Inclusion of a new procedure related to Sanctions Compliance in Section 22. • Expansion of Section 23 to include financial penalties for failure to comply with AML rules and for late submission of AML reports. • Changing the reference of the Compliance Directorate of CBB to the new name i.e. Anti-Financial Crime Department. • Amendment of the appendices to remove images of the account opening form, KYC form etc. and inclusion of a documentation checklist. • Adding UGB's Bank Code (# 30 – UNIT) to all responses affirming the absence of accounts for

			individuals / entities specified by the CBB in its circulars. A template of the response (as specified by the CBB) is introduced in Appendix 7. UNIT) as per our records