



თიბისი | TBC


P

PLC

3rd

# ANTI-FINANCIAL CRIME POLICY



<b>Target audience:</b>	Group Companies	
<b>Policy Owner (Responsible for the document):</b>	Compliance Department of TBC Bank JSC	
<b>Units engaged in the implementation:</b>	CEOs/Management boards of the Group Companies	
<b>Reviewed by:</b>	TBC Bank Group PLC Board of Directors   <hr/> Arne Berggren Chairperson of the TBC Bank Group PLC Board	
<b>Approved by:</b>	TBC Bank Group PLC Board of Directors	
<b>Effective Date:</b>	19.05.2025	
<b>Replaces (Previous version):</b>	N/A	
In the event of any discrepancies between the English version of this Policy and a translated version, the English version shall prevail.		
<b>Version</b>		<b>Date</b>
<b>Current version</b>	3 <sup>rd</sup>	19.05.2025
<b>Revision frequency</b>	Annual/Ad hoc	
<b>Accessibility</b>	Internal	
<b>Application</b>	All Group Companies must adhere to this Policy in its entirety. If a Group Company wishes to adopt and modify its content, it may do so as long as the modifications do not contravene the intent of this Policy. Otherwise, any changes made require approval from TBC Bank Group PLC Board of Directors.	
<b>Implementation</b>	In order to implement this policy, Management adopts the relevant procedures / guidelines that should be established in alignment with the rules outlined by Subsidiary Governance Procedure.	
<b>Definitions</b>	Terms written in bold capital letters that have not been defined in this Code will carry the same meanings as stated in the Glossary approved by TBC Bank Group PLC Board of Directors	

## Table of Contents

1. PURPOSE AND SCOPE	4
2. FINANCIAL CRIME RISK MANAGEMENT FRAMEWORK	4
3. RISK APPETITE STATEMENT	5
3.1. Restrictions and Prohibitions	5
3.2. Enhanced Controls	6
4. ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM	6
4.1. AML Function	7
4.2. Defense Lines within AML/CFT	7
4.3. Know Your Customer (KYC), Know Your Partner (KYP), Know Your Employee (KYE)	7
4.3.1 KYC	7
4.3.2 KYP	8
4.3.3 KYE	8
4.4 Correspondent Relations	8
4.5 Due Diligence and Confidentiality	9
5. ANTI-BRIBERY, ANTI-CORRUPTION AND ANTI-FACILITATION OF TAX EVASION	9
5.1. Minimum Standards	9
5.2. Hospitality and Gifts	10
5.3. Donations and Sponsorship	10
5.4. Facilitation Payments	11
5.5. Facilitation of Tax Evasion	11
6. MONITORING OF TRANSACTIONS AND REPORTING	12
7. SANCTIONS	13
7.1. Principles of Sanctions Regimes Application	13
8. OTHER TERMS	16
8.1. Record Keeping and Accounting	16
8.2. Employee Training Programs	16
8.3. Raising The Concern	16
8.4. Responsibility	16

## 1. PURPOSE AND SCOPE

- 1.1. The purpose of this **Policy (Policy)** is to assume responsibilities of **TBC** to protect its customers, shareholders and society from **Financial Crime**, other improper actions and any resulting threat. Therefore, the **Policy** is to set out the general principles/approach for **Financial Crime Risk** management and compliance standards in **TBC**.
- 1.2. The **Policy** is designed to ensure that **TBC** adheres to applicable laws and regulations in relation to **Financial Crime** compliance for the jurisdictions in which it operates as well as with relevant sanctions regimes.
- 1.3. The aim of the **Policy** is to establish effective systems and adequate internal control mechanisms and to set relevant requirements and responsibilities of the **Group Companies** to mitigate **Financial Crime**. This **Policy** covers following topics:
- **Financial Crime Risk** management framework – the obligation of **TBC** regarding risk management;
  - Risk appetite statement – **TBC's** responsibility for the determination of risk exposure and the implementation of strategies to mitigate those risks;
  - **AML** requirements and combating terrorism – **TBC's** obligation on development of sophisticated due diligence plans or procedures for assessment of **Money Laundering** risks and detection of suspicious transactions as well as obligation on assurance of compliance with relevant applicable legislative requirements or relevant standards;
  - Anti-Bribery, anti-corruption and anti-facilitation of **Tax Evasion** – **TBC's** obligation to prevent **Bribery** and **Corruption** by having adequate procedures to monitor and identify where and when it may occur;
  - Sanctions – **TBC's** obligation to meet applicable international and/or local sanctions.
- 1.4. The **Policy** provides rules on the types of behavior that may give rise to violations of applicable laws and requirements and reinforces a culture of honesty and openness among **TBC**. The **Policy** is also to set out behavior that is expected of **Employees** and **Management** and any person acting on **TBC's** behalf and is to provide a common standard of good practice across **TBC**.
- 1.5. **Management** of the **Group Companies** adopts detailed procedures in accordance with this **Policy** as well as in accordance with the applicable legislation and standards.
- 1.6. For the purposes of this policy, local legislative definitions shall apply. In cases where a term is not defined under local regulations, the definition provided by the Financial Action Task Force (FATF) shall be used.

## 2. FINANCIAL CRIME RISK MANAGEMENT FRAMEWORK

- 2.1. **TBC's Financial Crime Risk** management framework is aimed to ensure effective processes for enterprise and group wide risk management and is to be promoted and maintained across all areas of **TBC**. It also promotes the prompt resolution of issues through open escalation channels.
- 2.2. **Financial Crime Risk** management framework is integral part to all aspects of the **Group Company** activities and is the responsibility of all **Employees** to obey. **Management** has a particular responsibility to evaluate their risk environment, to put in place appropriate controls and to monitor the effectiveness of those controls in accordance with this **Policy** and applicable standards.
- 2.3. The framework adopted includes:

- Clearly allocated accountabilities and responsibilities to manage **Financial Crime Risk**;
- A strategy for actively promoting a strong anti-financial crime compliance culture;
- Governance structure that sets out appropriate mandates, authorities and oversight capabilities; and
- Adequate resources in respect of personnel, competency and technology.

2.4. In conformity with international best practices **TBC** also implements standards that are stricter and puts in practice approach according to which any discrepancy between **TBC** standards and domestic legislative requirements shall be considered in a following way:

- If the domestic legislation is stricter than **TBC** rules, the domestic requirements shall take precedence, and **TBC** rules must be promptly revised to ensure compliance.
- If **TBC** rules are stricter than the domestic legislation, **TBC** rules must be followed;
- If **TBC** rules contradict with the domestic legislation, relevant information must be submitted for the consideration to **Compliance Function** and the latter is to clarify, analyze and take relevant measures as per domestic legislation or internal requirements.

### **3. RISK APPETITE STATEMENT**

**TBC** has zero tolerance for **Financial Crime**, regulatory breaches and any attempt to circumvent **TBC's Financial Crime** policies and controls. **TBC** adheres to the following core principles:

- To show zero tolerance for facilitation of **Financial Crime** and fraud;
- To ensure not conducting business with individuals or entities believed to be engaged in an inappropriate and unlawful activity;
- To avoid risks that could jeopardize **TBC's** strategic plans, including activities that could make **TBC** vulnerable to any type of public or private litigation or enforcement that could be damaging to **TBC's** reputation and cause deterioration of relationship with regulators;
- To prohibit or cease operating of any product/service or customer segment line, for which the management believes that **TBC's** control mechanisms cannot protect **TBC** from risks that exceed the tolerance threshold;

In adherence to the following principles, **TBC** is dedicated to engaging in business with reputable customers and counterparties. Henceforth, illicit activities involving customers or contractors are deemed unacceptable for **TBC**.

To strengthen efforts towards customer relationships and to detect questionable or unusual behavior, **TBC** employs appropriate technological resources as well as various strategies executed by **Employees**.

#### **3.1. Restrictions and Prohibitions**

3.1.1. **TBC** is committed to conduct business with reputable customers and counterparties. Therefore, **TBC** has no risk appetite for customers and contractors who are engaged in any illegal activity. **TBC** does not serve and does not have business with persons/entities, if it has information or suspicion that they:

- Are involved in or associated with illegal manufacturing and trading of weapons, arms and munitions;
- Are involved in financing of proliferation of weapons of mass destruction;

- Are involved in or associated with human trafficking, illegal production and distribution of drugs, creation and distribution of pornographic products, smuggling or other criminal activity;
- Are engaged in any field of regulated activity without having appropriate permission/license;
- Are perpetrators of tax crimes;

3.1.2. It is also prohibited:

- To establish/maintain business relationship with shell banks;
- To open and maintain nested accounts, which allow transactions initiated by financial institutions who are customers of respondent financial institutions;
- To open and maintain payable through accounts which means an account of the respondent bank which is accessible directly by a third party to effect transactions on its own behalf.

### **3.2. Enhanced Controls**

**TBC** has enhanced controls in relation to types of industries and jurisdictions as set out below (non-exclusive list) and reserves the right to restrict activities in relation to:

- Businesses related to forex/binary option;
- Businesses related to virtual assets;
- Cash intense businesses;
- Payment service providers/money transmitters;
- Companies registered in offshore jurisdictions;
- Shell and shelf companies;
- Companies registered in free industrial zones;
- Companies with no operational connection to the country of operation of **Group Company**;
- Companies incorporated in or with connections/major counterparties to jurisdictions with increased risk;
- Non-residents without the reasonable purpose of holding business with the **Group Company**;
- Gambling companies (except of skilled-based games);
- Business related to antiques, precious stones and metals;
- Business related to firearms (including hunting equipment);
- Companies that issue bearer shares (except of listed companies);
- Political organizations;
- Charities;
- **PEPs** and companies under **PEPs** control;
- Other persons the service of which places a significant **Money Laundering** and reputational risk on **TBC**.

## **4. ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM**

**TBC** has in place relevant policies and procedures to fight against **Money Laundering**, **Terrorism Financing** and any other activity related to **Financial Crime**.

**Anti-Money Laundering (AML)** and **Combating the Financing of Terrorism (CFT)** Policies are developed based on the international standards and in accordance with the domestic regulations of countries where **TBC** performs its activities. It applies to all **Group Companies**, especially those that are **AML/CFT** designated entities, their branches, units and **Employees**.

#### **4.1. AML / Sanctions control Function**

The **AML/Sanctions control** function of the **AML/CFT** designated entities within **TBC** is the executive and policy making body who is in charge of implementing the **AML/CFT** and sanctions policies. **AML/Sanctions control** function, in accordance with this **Policy** and relevant procedures:

- Coordinates the monitoring process within the **AML/CFT** designated entity;
- Independently and with right to veto takes the decisions regarding **AML/CFT/Sanctions** matters;
- Has the right to immediately receive any information related to any customer and transaction as well as the right on confidentiality of their information.

#### **4.2. Defense Lines within AML/CFT/Sanctions control Function**

4.2.1. Risks related to **AML/CFT/Sanctions** is managed through three lines of defense.

4.2.2. The first line of defense is ensured by all **Employees** of **TBC**, who are responsible for implementation and compliance with **AML/CFT/Sanctions** policies and procedures.

4.2.3. The second line of defense - **TBC** and **Group Companies** have autonomous dedicated **Employees** to perform **AML/CFT/Sanctions** control works whose decisions regarding the topics under their responsibility may not be overridden.

4.2.4. The third line of defense (Internal Audit) provides objective and independent assurance. While the third line's key responsibility is to assess whether the first and second-line functions are operating effectively, it is charged with the duty of reporting to the **Supervisory Board** (Audit and/or relevant committee at the **Supervisory Board**), in addition to providing assurance to regulators and external auditors that the control culture across **TBC** is effective in its design and operation.

#### **4.3. Know Your Customer (KYC), Know Your Partner (KYP), Know Your Employee (KYE)**

Sound **KYC**, **KYP** and **KYE** procedures have particular relevance to the safety and soundness of **TBC**.

While constituting an essential part of sound risk management, **KYC**, **KYP** and **KYE** help to protect **TBC's** reputation and the integrity by reducing the likelihood of **TBC** becoming a vehicle for or a victim of **Financial Crime** and/or suffering consequential reputational damage.

Intermediaries ought to be maintained solely on the premise of acquiring essential services and only if every interaction with external parties is recorded.

##### **4.3.1 KYC**

4.3.1.1 **TBC** has in place relevant **KYC** Procedures which are part of internal control rules of **TBC** and therefore, **Employees** are required to know their customers. **TBC** observes **KYC** obligations and due diligence requirements and identifies it as:

- An essential part of risk management;
- The tool for **TBC** to be prevented from being involved in or used for illegal activities;
- The tool for mitigation of risks damaging **TBC's** reputation.

4.3.1.2 In accordance with applicable legislation, **AML/CFT** policies and procedures and relevant standards, **TBC** assesses customers' risk level from the **ML/TF** and sanctions risks point of view through following three risk categories – low, standard and high. Such assessment allows **TBC** to use risk-based approach and therefore implement proportional measures and resources for the prevention of **Money Laundering, Terrorism Financing**, violation of sanctions regimes and/or any other **Financial Crime**.

4.3.1.3 The customer risk level is initially determined at the moment of establishing business relationship and is subject to reviewing throughout the whole period of business relationship on a periodic or ad-hoc basis.

#### **4.3.2 KYP**

4.3.2.1. Reasonable due diligence process is undertaken by **TBC** before it enters into any relationship with any third party in particular:

- A **Financial Organization** or any partner (any entity that may enter into one time or continuous business relationship);
- A vendor, or outsource company, or supplier.

4.3.2.2. Within the **KYP** policies and procedures **TBC** ensures that any partner and its structure, as well as its **UBOs** are properly determined and screened.

4.3.2.3. Selection and evaluation of vendors is performed in accordance with the applicable procurement procedures ensuring the exclusion of possible cases of **Corruption** as well as any type of reliance with **Financial Crime**.

4.3.2.4. The procedures relating to the procurement of goods and services from external service providers, vendors and similar third parties are conducted with bidding processes and according to the “arm’s length” principle.

#### **4.3.3 KYE**

4.3.3.1. **TBC's KYE** procedures cover both pre-contractual and post-contractual relationship with the **Employees**. **KYE** allows each **Group Company**, with high care and careful examination, to understand **Employee's** background, conflicts of interest and vulnerability to **Financial Crime, Money Laundering** complicity. **KYE** also ensures compliance with **TBC's** corporate culture, ethical norms and any other applicable requirements.

4.3.3.2. As part of **KYE** program monitoring process **TBC** identifies **Employees'** suspicious activity to prevent the possible breach of regulatory requirements, reputational damage and/or financial loss.

#### **4.4 Correspondent Relations**

4.4.1. **TBC** has implemented measures for effectively managing correspondent relations and have relevant prohibitions in place. The term “correspondent relations” is used here in a broad sense and includes correspondent banking relations and similar relations of other **AML/CFT** designated entities, for example, with:

- Reinsurance companies or insurance brokers;
- Payment service providers;
- Companies engaged in financial instruments' market;
- Financial institutions providing credit facilities;



4.4.2. Terms on establishment and maintenance of correspondent relationships, as well as related prohibitions within **AML/CFT** (i.e., suspension of transactions or services, etc.), are regulated by specific internal regulations of **Group Companies** depending on their needs and legislative requirements.

#### **4.5 Due Diligence and Confidentiality**

4.5.1. Based on the customer risk level **AML/CFT** designated entities introduce simplified, standard or enhanced due diligence methods.

4.5.2. **Customer Due Diligence (CDD)** measures include:

- Customer identification and verification (including persons authorized to act on behalf of customer, ultimate beneficial owners, controlling and other relevant persons);
- Screening against the lists (sanctions, **PEPs**, enforcement, etc.);
- Update of identification data/documentation;
- Risk classification/reclassification of customer;
- Monitoring of transactions;
- Obtaining additional information where necessary.

4.5.3. **TBC** ensures the confidentiality of any information obtained through any processes in accordance with applicable legislation, international standards and the best practices.

4.5.4. **TBC** treats any confidential information with the highest care, considering it as the most valuable asset and has relevant information security, confidentiality and personal data protection policies and procedures.

### **5. ANTI-BRIBERY, ANTI-CORRUPTION AND ANTI-FACILITATION OF TAX EVASION**

**TBC** prohibits any form of **Bribery** and corruption, including but not limited to accepting, offering, paying, giving, soliciting or authorizing bribes, by promoting internal integrity and fulfilling the obligation towards the stakeholders of **TBC** by adhering to any and all applicable legislation and standards.

**TBC** has no appetite for any **Fraud** or **Corruption** committed by, or any appearance of **Fraud** or corruption, shown by its **Employees** or third parties acting on behalf of any **Group Company**.

**TBC** takes all facts of suspected **Fraud** or **Corruption** very seriously and responds fully and fairly. Therefore, the prevention, detection and reporting of any forms of **Corruption** and **Fraud** is the responsibility of all **Employees**.

#### **5.1. ABC Policy Framework**

ABC policy framework is structured in three levels:

- Level 1  
Board level Policy: Anti- Financial Crime Policy – covering ABC statement and underlining **TBC's** commitment towards ABC compliance
- Level 2  
Detailed procedures related to the implementation of the requirements included in the Anti-Financial Crime Policy
- Level 3

Procedures and methodologies: Procedural documentation in relation to level 1 or level 2 policies or procedures

## **5.2. ABC Core Statements**

5.2.1. **TBC** has in place clearly defined anti-bribery rules, effective controlling systems, internal mechanisms for promoting integrity, a well-defined remuneration policy and management of conflicts of interest and accountability rules.

5.2.2. **TBC's** anti-bribery, anti-corruption and anti-facilitation of **Tax Evasion** program (**ABC**) covers the following components:

- Tone at the top/ governance support;
- Policies and procedures;
- Business processes risk assessment (including third-party due diligence);
- Communication and awareness;
- Enforcement and sanctions;
- Reports and investigations;
- Disclosure procedures;
- Implementation of proper financial controls;
- Clear definition of prohibited behavior.

## **5.3. Hospitality and Gifts**

5.3.1. TBC ensures that all permitted gifts and hospitality and travel and accommodation, given or received, from third parties, are not given or received in exchange of an improper advantage for the benefit of TBC, its employees, third parties or any other persons or entities, and are in compliance with the internal procedures, including recording in the Register and threshold for acceptance.

5.3.2. The **Policy** doesn't prohibit bona fide hospitality and promotional or other business expenditure which seeks to:

- Improve the image of **TBC**;
- Better to present products and services; or
- Establish cordial relations.

5.3.3. The general **Bribery** offences pertain to those situations where it is considered that offering or receiving hospitality might influence, or be perceived to influence, a business decision or a person to act improperly. For such cases, **TBC** has in place relevant procedures and policies including, the Code of Conduct and Ethics.

## **5.4. Sponsorship, Donations, Charitable Contributions**

5.4.1. TBC ensures that sponsorships, donations, charitable contributions are not to be offered, provided or accepted in exchange for obtaining or retaining an improper advantage for the benefit of TBC, its employees, third parties or any other persons or entities, and are in compliance with the internal procedures on vetting and approval

5.4.2. **TBC** may support local charities or provide sponsorship of certain programs such as social, cultural or sporting events, but in obedience to legal and internal procedures, which include the following:



- **TBC** conducts appropriate due diligence on and provide donations to organizations/persons that serve a legitimate public purpose, and which are themselves subject to high integrity standards;
- **TBC** has a clear and transparent approach to charitable organizations, including the selection process of suitable recipients considering respective risks;
- The risk of all charitable donations made in **TBC's** name, as well as the risk of recipients are assessed by the **Compliance Function** before the **Management Board** approval;
- **TBC** identifies any political connections (for example Ultimate Beneficial Owner (**UBO**), controlling persons) of a charitable organization and if there are any, continue the activity according to applicable policies and procedures.

5.4.3. All processes related to the selection, risk assessment and approval/denial procedures of donations to charitable organizations are documented.

5.4.4. **TBC** does not make donations to any political parties or organizations. All charitable donations when the recipient is connected to **PEP**, public officials, organizations or individuals engaged in politics must be approved by the **Group CEO**.

## 5.5. Third Party Risk Management

5.5.1. TBS carries out a risk assessment before entering into a relationship with a third party, including for acquisitions, mergers and joint ventures, and applies due diligence measures on a risk-based approach in line with the Procurement Policy and Outsourcing Policy. The assessment may include background checks, financial audits, reputation checks, and compliance history of the third party, as relevant in function of the relationship with TBC, and is updated on a periodic basis.

## 5.6. Hiring

5.6.1. TBC ensures that all offers of employment, whether permanent or temporary are fair, transparent, merit-based and in line with the Human Resources Requirements, specifically in relation to candidates related to public officials. TBC screens candidates on adverse media to detect potential bribery or corruption background

## 5.7. Facilitation Payments

5.7.1. Facilitation payments are unlawful payments made to the public or government officials to secure or expedite routine or necessary official action, either more promptly or at all. **TBC** and its **Employees** must not be engaged in facilitation payments.

5.7.2. For these purposes of present **Policy**, payments to governmental entities (in the form of official fees and charges) required under relevant law, rules or regulation which are lawfully documented are not considered to be facilitation payments.

## 5.8. Facilitation of Tax Evasion

5.8.1. **TBC** has and is to have zero tolerance for **Tax Evasion** or the facilitation of **Tax Evasion**. **TBC** will not tolerate any of Employees, agents or business partners knowingly assisting or encouraging **Tax Evasion**.

5.8.2. **TBC** is strongly committed not to be engaged in transactions aimed at or somehow related to **Tax Evasion**.

## **5.9. Internal Controls**

- 5.9.1. TBC establishes appropriate internal control system, including accounting controls to track payments and expenses, and compliance checks into existing processes and controls

## **5.10. Reporting and Escalation**

- 5.10.1. TBC ensures that any employee or third party who knows or suspects a bribery or corruption risks or has knowledge of bribery or corruption that has occurred or that an attempt may occur or is being attempted by a colleague, a customer, a business counterpart or any other third party, notifies immediately TBC. TBC ensures that multiple channels of escalation are available to the employees, including email and web-based means and ensures anonymity and protection of whistle blowers against retaliation.

## **6. MONITORING OF TRANSACTIONS AND REPORTING**

- 6.1. **TBC** performs monitoring over transactions, deals, and relations performed by their customers and/or partners through its systems, channels or tools. The purpose of monitoring is:
- To prevent the involvement of **Group Companies** in illegal activities, including **Money Laundering** and **Terrorism Financing, violation of applicable sanctions regimes**;
  - To prevent illegal activities of customers (including carrying out transactions aimed at **Money Laundering, Terrorism Financing and violation of applicable sanctions regimes**);
  - To prevent violation or avoidance of applicable sanctions;
  - To detect transactions which according to domestic legislation are subject to reporting to local Financial Intelligence Units (FIU) or other relevant authorities.
- 6.2. **TBC** pays special attention to unusual transactions, which do not have visible economic (commercial) content or lack lawful purpose, ascertains the purpose and grounds of such transactions to a reasonable extent, and documents the results obtained.
- 6.3. **TBC** has a methodology for identifying, assessing, managing and communicating **ML/TF/Sanctions** risks the organization is facing. The risk factors used to define the organization's **ML/TF/Sanctions** risk include, but are not limited to the following factors:
- Field of activity, structure and model of the business;
  - Geographical risk;
  - Products, services and channels of delivery;
  - Structure of customer base;
  - Customer Status;
  - Identity of **UBOs**;
  - Transactions of customers;
  - Risk mitigation measures and resources, which are in use;
  - Assessment of supervisory authority and fulfillment of respective recommendations.

- 6.4. The mentioned list is not exclusive and therefore **TBC** conducts its activities in accordance with applicable laws as well as relevant standards.

## **7. SANCTIONS**

Sanctions are a policy tool that national governments, such as the **US** and the **UK**, and multinational organisations, including the **UN** Security Council and the Council of European Union, use in order to constrain and deter perceived security threats to prevent or suppress criminal activity or to encourage change in or to apply pressure on a target country or regime. Sanctions can therefore take the form of any of a range of restrictive or coercive measures. Failure to comply with these obligations can carry significant consequences for **TBC**.

**TBC** prohibits and will not facilitate activity with certain governments, countries and regions, entities and sectors of activities that are subject to relevant sanctions programs. **TBC's** activities are formed on the basis of laws, regulations, regulatory guidance and trends in sanctions and enforcement under the regulatory regimes imposed by or under:

- Domestic legislation and/or by local authorities.
- The United Nations (**UN**) through the United Nations Security Council in relation to economic, financial and trade sanctions;
- The European Union (**EU**) through the Council of the European Union;
- The United States Treasury Department, through the Office of Foreign Assets Control (OFAC);
- The United Kingdom (**UK**), through the Office of Financial Sanctions Implementation HM Treasury.

**TBC** takes into consideration the standards set by the Basel Committee, the Wolfsberg Group, and the European Banking Authority. Together with the rest requirements, all **Group Companies** are strictly prohibited to enter into business relations or provide services to persons, which are under sanctions established by UN Security Council Resolution #1373 (2001) and any other related resolutions.

### **7.1. Principles of Sanctions Regimes Application**

- 7.1.1. Compliance with sanctions regimes is contingent upon the specific requirements and organizational structure of the **Group Company**. As a result, certain requirements must be fulfilled in different ways depending on those factors.
- 7.1.2. **Group Companies** must act in compliance with the applicable sanctions related laws and regulations if the following conditions simultaneously apply:
- Various **UK, EU** or **US** nationals are present in the **Supervisory** or **Management Board**; and
  - **Group Company** cannot release those **UK, EU, or US** nationals from their duties to approve, or in any way participate in, any transactions with countries, companies, or individuals that are targeted under the respective **UK, EU, or US** sanctions regimes/ programs;
- 7.1.3. Nevertheless, if the cumulative conditions provided in clause 7.1.2. are not applicable, the **Group Companies** must conduct business in compliance with the economic and trade sanctions laws and regulations of the **UN, UK, EU, US** and any other government or authority with jurisdiction over the **Group Company** activities, where the underlying activity or transaction triggers applicability of sanctions regulations of **UK, EU** and/or **US** jurisdiction(s) by means of any aspect of such activity or transaction, such as the use of **UK, EU** and/or **US** currencies or financial institutions, creating a nexus and engagement with the **UK, EU** and/or **US** jurisdiction(s).

- 7.1.4. Any activity or transaction falling outside the scope of the events provided in clauses 7.1.2. and 7.1.3 is to be further assessed by the acting legal entity of **TBC** having full discretion and decision-making power taking into account the applicable domestic laws and regulations.
- 7.1.5. **TBC** considers the following countries and regions as being subject of a comprehensive sanctions regimes/program and applies the relevant restrictions: Cuba, Iran, North Korea, Syria and the regions of Crimea and occupied territories in Ukraine and Georgia.
- 7.1.6. In contrast to **Financial Institutions**, **Group Companies** that are not classified as **Financial Institutions**, as per applicable regulation, have the option of conducting screenings through due diligence and **KYP** processes/procedures. This enables them to evaluate potential risks and ensure compliance with regulatory requirements.
- 7.1.7. As per applicability for non-financial **Group Companies**, but as a must for **Financial Institutions**, in accordance with relevant regulations, it is important to thoroughly evaluate and review all parties involved, including related individuals, transactions, agreements, external entities. This screening process should encompass various aspects such as clients (including occasional or intermediate shareholders), beneficial owners, directors, authorized signers, attorneys and their authorities. Additionally, guarantors associated with business relationships need to be assessed along with any other connected activities or transactions like payments arrangements for trade finance. It is crucial that this evaluation extends not only to providers but also agents or intermediaries who may have a role in these dealings. Compliance measures must also account for the assessment of **Employees** alongside any other pertinent third parties in order to ensure thorough due diligence. Transactions conducted with the local currency are exempt from payment screening according to domestic regulatory standards. However, **Financial Institutions** must ensure that their customers undergo screening against relevant sanctions regimes such as those imposed by the UN, UK, EU and US or any other applicable authorities.
- 7.1.8. Considering the abovementioned statements and principles:
- 7.1.8.1. Screening is done at on-boarding and on an ongoing basis. In order to ensure effective screening throughout the duration of the relationship, any modifications or additions made to sanctioned lists or customer data must be promptly incorporated within a maximum timeframe of 24 hours. This ensures that updated information is utilized expeditiously for the purpose of evaluating and monitoring potential risks associated with customers.
- 7.1.8.2. **TBC** must define and implement adequate screening tools, including fuzzy-logic, and must assess its effectiveness and efficiency regularly. **Financial Institutions** must screen all applicable transactions in real-time before the transaction is executed, against relevant sanctions lists.
- 7.1.8.3. **TBC** makes sure all appropriate counterparty and transaction due diligence is conducted, before entering into any international trade finance operation or before processing any related payments, in order to mitigate the risk of violating any applicable international sanctions programs and/or restricted goods and merchandise regulations, including dual-use goods.
- 7.1.8.4. **TBC** does not recruit or hire **Employees** or enter into or maintain relationships with third party service providers, landlords and tenants, who are named on a sanctions regulatory list or who are permanently resident in a country under a comprehensive sanctions program.
- 7.1.8.5. **TBC** establishes appropriate processes and procedures to review and refresh sanctions lists on a regular basis.
- 7.1.8.6. **TBC** establishes processes to block, freeze, reject and return financial transactions that are restricted or prohibited under applicable sanctions regimes, as well as transactions involving countries under a

comprehensive program and/or sanctioned entities or individuals to the extent required by applicable regulations. **TBC** therefore blocks or freezes accounts and/or other property of sanctioned individuals or entities who maintain a customer relationship immediately when detected. **TBC** will report to the relevant authorities if required and if applicable to **TBC**.

- 7.1.8.7. **TBC** defines and implements adequate controls to prevent attempts of sanctions circumvention by customers, employees or any third party.
- 7.1.8.8. **TBC** makes sure to include sanctions clauses in all account opening, trade contracts and other transaction agreements to ensure compliance with this **Policy** and with associated policies and procedures.
- 7.1.8.9. **TBC** ensures sanctions processes and procedures are in place to report as applicable and to respond promptly to regulatory requests, as well as in relation to third party requests as applicable and allowed by domestic regulations.
- 7.1.8.10. **TBC** appoints a dedicated **Employee(s)** within the **Compliance Function** with appropriate level of responsibilities and authorities in relation to implementation of Sanctions related matters, and ensures that sufficient resources are provided.
- 7.1.8.11. **TBC** implements and maintains procedures and controls to ensure that any potential sanctions match or any transaction or series of transactions requiring a “Specific License” or subject to a “General License” is immediately escalated to the **Compliance Function**.
- 7.1.9. **TBC Employees** who are **UK, EU or US** persons must not approve, or in any way facilitate, any transactions with countries, companies, or individuals that are designated, sanctioned and targeted under the respective **UK, EU or US** sanctions program or are being owned or controlled by such **UK, EU or US** designate, sanctioned and targeted companies or individuals. **Employees** who are **UK, EU or US** persons must not be requested or expected to provide guidance on transactions for any members of **TBC** where a risk of "facilitation" exists.
- 7.1.10. **Financial Institutions** conduct an annual business risk assessment of sanctions risks and the effectiveness of sanctions controls throughout **TBC**.
- 7.1.11. **Financial Institutions** establish appropriate key risk indicators and monitoring measures to assess ongoing compliance as per the requirements set out within this **Policy**, including but not limited to:
- Customer on-boarding and ongoing monitoring measures;
  - Customer screening controls;
  - Transaction filtering controls;
  - List management processes;
  - Payment stripping and resubmission controls.
- Other prohibitions and restrictions arising from various sanctions regimes are established by internal regulations of **Group Companies** in accordance with domestic legislation, requirements of sanctions, identified risks and resources to manage those risks.
- 7.1.12. In keeping with best practices and as a component of adherence to regulations, it is necessary for both **Management** and **Employees** to actively supervise the imposition of relevant sanction systems. In cases requiring the interpretation of matters pertaining to sanctions, sanction nexus, sanction clauses, deals or transactions, as well as counterparties, unless in contradiction with present **Policy** and applicable



regulations/standards, **Management** and **Employees** must seek assistance from **TBC JSC's** Compliance Department and General Counsel/Head of Legal Department.

## **8. OTHER TERMS**

### **8.1. Record Keeping and Accounting**

8.1.1. **Group Companies** shall record and keep the information/documentation on customers, beneficial owners, associated entities obtained from various sources, information on transactions (operations) performed by them as well as other relevant information determined under this **Policy** electronically and/or materially in accordance with applicable legislation.

8.1.2. **Employees** must act in accordance with applicable standards, principles, laws and policies for accounting and financial reporting and maintain accurate books and records in accordance with applicable regulatory and legislative requirements.

8.1.3. Detailed rules on record keeping and archiving of documents are defined by internal regulations of the **Group Companies**.

### **8.2. Employee Training Programs**

8.2.1. Training is obligatory and applies to new and existing **Employees** at all levels. **Group Companies** shall ensure that all their **Employees** are well trained and enabled to identify conspicuous occurrence indicating **Money Laundering, Terrorism Financing** or other illegal activities.

8.2.2. In order to comply with and fulfill the requirements of the local and international trends in anti-financial crime activities, relevant specialists/**Employees** shall regularly attend external and/or internal trainings dedicated to respective areas in accordance with applicable policies and procedures or applicable legislation.

8.2.3. Present **Policy**, where appropriate, is to be disclosed to third parties and is clarified that all activities carried out on behalf of **TBC** must be in compliance with applicable law as well as with present **Policy**.

### **8.3. Raising The Concern**

8.3.1. Any material warning signs or red flags identified at any stage of the due diligence process must be addressed to the **Compliance Function** before employees proceed with any proposed arrangement.

8.3.2. An **Employee** should report at the earliest possible stage to the **Compliance Function** if there is any suspicion or observation related to anything that might be violation of this **Policy**.

8.3.3. **Employees** should raise their concerns to the **Compliance Function** of **TBC** at the e-mail [compliance@tbcGroup.com.ge](mailto:compliance@tbcGroup.com.ge) or report the information in accordance with the Incident Response Policy.

### **8.4. Responsibility**

8.4.1. To ensure the implementation of this **Policy** and assign appropriate accountabilities for any violations, also to exclude the criminal and/or civil responsibility as a result of any breach, it is important that **TBC** implements robust mechanisms.



- 8.4.2. Such mechanisms should be designed to effectively enforce compliance with existing policies by establishing clear guidelines for adherence and by holding individuals accountable in case of non-compliance.