BASISBANK

Approved
JSC "Basisbank"
By the Supervisory Board
January 08, 2025
Meeting minutes N08.01/01-25

Group Anti-Financial Crime Policy

BasisBank Group

January 2025

BASISBANK

Table of Contents

Introduction

The fight against financial crime is at the core of the BasisBank Group's (also referred to as "the Group", "BasisBank" or "BB Group") strategy and risk appetite. Financial crime risks encompass:

- **Money Laundering and Terrorist Financing**
  Money laundering or terrorist financing are a global challenge which has an incalculable economic and human cost on the society, and the Group recognises its fundamental responsibility to help trace and stop the financial flows linked to serious crime and terrorism, to protect the integrity and the sustainability of the financial system and make society safer.

- **Breaches and Circumvention of International Sanctions**
  Sanctions are a policy tool that national governments and multinational organizations use to deter perceived security threats and criminal activities or to apply pressure on a target country. Failure to comply with international sanctions and to control sanctions circumvention can bear significant regulatory and financial consequences on the Group and may impact relationships with Correspondent Banks.

- **Bribery and Corruption**
  Bribery and corruption carry a huge economic loss and inefficiency, poverty, intimidation and inequality. Additionally, it distorts markets, undermines fair access to employment on a merit-based and hinderes the achievability of the sustainable development goals. The Group acknowledges its responsibility to promote a fair and transparent environment to prevent bribery and corruption.

BasisBank is committed to fight against financial crime, to set up and to implement Anti-Financial Crime risk management programme (or AFC programme below) to identify, understand and mitigate the financial crime risks.

The AFC Policy establishes the minimum requirements set out by the Group, to mitigate potential compliance, regulatory and reputational risks associated with violations of Anti-Money Laundering and Counter Terrorism Financing (AML/CTF), International Sanctions and Anti-Bribery and Corruption (ABC) laws, regulations and international standards.

Regulatory Environment

Georgia is a member of Moneyval since 1999 and has enacted laws and rules designed to implement the AML/CTF recommendations of the Financial Action Task Force (FATF) and compliance with international sanctions. Georgia is also member of the Group of States against Corruption ("GRECO").

In Georgia, the Anti-Financial Crime principles and rules includes:

- Law on "Facilitating the Suppression of Money Laundering and Terrorism Financing" last amended version dated June 28, 2023;
- Financial Monitoring Service of Georgia (FMS) Regulation on Approval of the Procedure of Identification and Verification of a Customer by Obliged Entity, June 5, 2020;
- FMS Regulation on Approval of the Rule on Record-keeping, Storage and Reporting of the Information on the Transaction by Obliged Entity to the FMS, June 5, 2020;
- National Bank of Georgia (NBG) Guidelines on the implementation of preventive measures n.4/04, January 12, 2021;
- NBG Guidelines for the Money Laundering and Terrorist Financing Risk Assessment, n. 82/04, May 7, 2019;
- NBG Guidelines in relation to compliance with international sanctions;
- Criminal Code establishing Anti-Money Laundering (AML) predicate offences and Counter Terrorism Financing (CTF) offences, and providing respective sanctions;
- Law on Operative-Investigative Activities by law enforcement authorities;

- Organic Law on the National Bank of Georgia

BasisBank is supervised by the National Bank of Georgia. In addition, the Group also takes into consideration the Standards set by the European Union (EU) Supervisory Authorities, the Basel Committee, the FATF and the Wolfsberg Group. In relation to International Sanctions, this policy is based on the laws and regulations issued by the United Nations Security Council (UN), the Council of European Union (EU), the Office of Foreign Assets Control (OFAC, US) and the Office of Financial Sanctions Implementation (OFSI) HM Treasury (UK).

Financial Crime Risk Definition

Financial crime is defined by BasisBank as:

- The conversion, transfer, acquisition, possession or use of property derived from criminal activity, or any type of participation in such activity (AML);
- The provision or collection of funds for terrorism financing (CTF);
- The services, directly or indirectly, provided to persons, entities, organisations, governments or countries subject to restrictive measures or asset freezing orders (International Sanctions);
- Any activity involving bribery and corruption (ABC).

AFC Policy Framework

The backbone of AFC programme is the AFC Policy Framework structured in three levels:

- **Level 1**
  Supervisory Board level policy: Anti-Financial Crime Policy (the present policy) covering the AFC Statements. The Risk Appetite Statement document is also a level 1 AFC Policy.
- **Level 2**
  Executive Board level policies: detailed policies related to the implementation of the requirements included in the AFC Statements.
- **Level 3**
  Procedures and methodologies: procedural documentation in relation to level 1 or level 2 policies.

The AFC Core Statements are the umbrella of this policy and apply to the three specific programs: AML/CTF, International Sanctions and ABC. It can be represented as follows:

AFC Core Statements		
AML/CTF Statements	International Sanctions Statements	ABC Statements

There is a total of 49 statements, which have been numbered to ease cross-reference with level 2 policies or policies from other functions:

- 7 AFC Core Statements, references AFC1 to AFC7
- 18 AML/CTF Statements, references AML1 to AML18
- 16 International Sanctions statements, references SAN1 to SAN16
- 8 ABC Statements, references ABC1 to ABC8.

AFC Core Statements

The following AFC Core Statements are overarching requirements applicable to each of the level 2 AFC policies, covering the understanding and assessment of the AFC risks, proper governance arrangements, three lines of defence and adequate internal control systems.

AFC Core Statements	
AFC1	**AFC Enterprise Wide Business Risk Assessment and Risk Appetite** The Group develops and maintains a thorough AFC risk assessment to identify, understand, manage and mitigate inherent AFC risks. Risk mitigation measures are designed and implemented to control adequately and effectively those inherent risks. Inherent and residual risks are managed in line with the Group's risk appetite.
AFC2	**Customer Acceptance Policy** In line with the AFC risk assessment and risk appetite, the Group defines and implements a customer acceptance policy outlining prohibited and restricted customer types and activities.
AFC3	**Supervisory Board** The Supervisory Board has a clear understanding of the AFC risks, oversights the AFC risk management programme and its effectiveness; and is responsible for setting the proper tone from the top.
AFC4	**Executive Board and AFC Related Committees** The Supervisory Board allocates explicit roles and responsibilities in the Executive Board, Senior Management and AFC decision making bodies. The Executive Board appoints dedicated staff members with appropriate level of responsibilities and authorities in relation to the AFC programme management and ensures that sufficient resources are provided.
AFC5	**Three Lines of Defence** The Group defines and implements an AFC operating model including the internal organisation with roles and responsibilities across the three lines of defence to ensure an effective AFC risk management.
AFC6	**Robust and Effective AFC Programme** The Group ensures that a robust and effective AFC programme is in place, covering: • Regulatory surveillance on new or updated regulations, industry standards and trends; • Documented and duly approved policies, procedures and methodologies; • Effective control processes on each key requirements, with the adequate internal control systems (AFC7) • Strong company culture, constant communication from the Board, AML/Sanctions Compliance department and Compliance Unit on AFC topics, and a regular training program on all AFC risks and requirements; • Monitoring via Key Risk Indicators (KRIs), quality assurance and testing performed by the second line of defence on key processes and controls; • Reporting and escalation to relevant functions and committees, to ensure oversight by the Executive Board and Supervisory Board; • Regular audit by the third line of defence, considering all AFC inherent risks; and • Adequate record-keeping processes, in line with local requirements.
AFC7	**Adequate Internal Control System** The Group has internal organisation and systems that are adequate with respect to its size, activities and complexity as well as with the AFC risks. Internal control system includes at least the following: • System(s) to record and maintain Know Your Customer (KYC) information for all relevant parties; • System(s) to perform and maintain the Customer Risk Assessment; • System(s) to screen clients and relevant parties from AML/CTF and international sanctions standpoints (screening versus lists and keywords);

	• System(s) to screen deals and transactions from AML/CTF and international sanctions standpoints, including sanctions circumvention (screening versus lists and keywords); • System(s) to monitor customer activity from AML/CTF and international sanctions circumvention standpoints (monitoring of the activity a-priori or post-factum); • System(s) to report and manage cases between the first and second line defences and the AML/Sanctions Compliance department, and between the AML/Sanctions Compliance Head and the relevant authorities; • System(s) to assess the Enterprise Wide Business Risk Assessment (AFC1); • System(s) to collect and maintain Key Risk Indicators.

AML/CTF Statements

The following AML/CTF Statements are requirements applicable to level 2 AML/CTF policies covering KYC, Transaction and Activity Monitoring and Suspicious Activity Reporting.

AML/CTF Statements	
AML1	**Compliance with AML/CTF Policy** The Group, and their employees, conduct business in accordance with applicable AML/CTF related laws and regulations, as described in the AML/CTF Policy.
AML2	**Predicate Offences** All predicate offences of the AML/CTF applicable regulations are duly covered by the AML/CTF policies, procedures and controls, including tax crime.
AML3	**Customer Risk Assessment (CRA)** All Group's customers and any business relationships are classified by money laundering and terrorist financing risk level at on boarding in function of an AML/CTF risk model. The customer risk assessment is reviewed on an on-going basis in function of the changes in the KYC information, the customer account activity, and the assessment of transactions screening and monitoring alerts.
AML4	**Customer Due Diligence (CDD) at On-Boarding** CDD is mandatory when on boarding a new customer or any business relationship. CDD is satisfactorily concluded before opening an account or providing a product or service to a new customer adopting due diligence measures commensurate with the risk perceived.
AML5	**Periodic and On-Going CDD Maintenance** CDD update is mandatory on a periodic basis in function of the risk level, at trigger events and at any time when the Group is aware that the relevant circumstances surrounding a business relationship have changed.
AML6	**PEP and Adverse Media** The Group ensures that customer which are Politically Exposed Person (PEP), related to a PEP, or with adverse media are detected during the CDD at on-boarding and on ongoing basis. The detection of PEP relation or adverse media for an existing customer is considered as trigger event, requiring an update of the CDD in line with AML4.
AML7	**Customer Acceptance** The Group does not accept customers or maintain relationships where the required data is not available, including for Beneficial Ownership, or when the customer falls into one of the Group's agreed categories of prohibited customers as per the Risk Appetite statement.
AML8	**Risk-Based Approach (RBA) and Enhanced Due Diligence (EDD)** Specific controls are implemented to exercise greater scrutiny over higher risk customers and transactions through Enhanced Due Diligence EDD measures, in line with a RBA.
AML9	**Correspondent Relationships** The Group does not provide Correspondent Banking services, and implements specific controls to oversight transactions processed as a respondent bank via its correspondent

	relationships network in order to mitigate appropriately the AFC risks, in line with international standards.
AML10	**Red Flags** All customer transactions are monitored for the purpose of identifying suspicious activity by determining red flags relevant to the Group, to the business line, to the product and to the customer risk and business profiles.
AML11	**RBA and Transactions Monitoring (TM)** The Group identifies and monitors from a risk-based approach and in an effective and comprehensive manner, any transaction made during a business relationship to ensure that they are consistent with the Group's knowledge of the customer.
AML12	**Transactions Monitoring System** All products offered to business relationships and all transactions types are monitored via an automated system for the purpose of identifying suspicious activities with the relevant red flags, including occasional transactions.
AML13	**Regulatory and Third Party Request** The Group maintains adequate systems and controls to respond timely and accurately to requests and notifications from the National Bank of Georgia, the Financial Intelligence Unit, other regulatory bodies and from key third parties.
AML14	**Tool System Calibration** The Group ensures that the tools used for transactions monitoring and reporting are assessed regularly to monitor and enhance, where necessary, effectiveness and efficiency of the control, by reviewing the scenarios and the calibration.
AML15	**AML Head Authority** The AML Head has the authority to refuse to open a relationship for a potential customer, to restrict the products, transactions or services offered to a customer, and to exit the relationship.
AML16	**Escalation to the AML Head** Any employee who has knowledge of any potential suspicious activity of Money Laundering/Financing of Terrorism (ML/FT) in the course of a business relationship or internally, escalates immediately a Unusual Transaction Report to the AML Head or to a designated employee.

AML17	**Reporting to the Financial Intelligence Unit** The AML/Sanctions Department Head or a designated employee reports to the Financial Intelligence Unit (FIU) – the FMS all transactions and activities deemed as suspicious on a timely basis. The AML/ Sanctions Compliance department monitors closely clients subject of report to FIU and assess if required to restrict or exit the relationship.
AML18	**Tipping-Off** All employees are prohibited from tipping off to the person concerned, or to a third party, when a report has been filed to the FIU, when an investigation is on-going or when relevant authorities have requested information.

International Sanctions Statements

The following International Sanctions statements are requirements applicable to level 2 International Sanctions policies covering customer screening and deals and transactions screening.

International Sanctions Statements	
SAN1	**Compliance with Applicable Sanctions Regulations** The Group, and their employees, conduct business in accordance with applicable sanctions-related laws and regulations, as described in the International Sanctions policy.

SAN2	**UN, EU, US and UK Sanctions Regimes** The Group conducts business in compliance with the UN, EU, US and UK sanctions regimes on the basis of the nexus of the customer, person, currency, transactions, goods and activities as defined by the EU, US and UK regulations, and by the local regulatory requirements.
SAN3	**EU, US and UK Persons** Group employees who are EU, US or UK persons do not approve, or in any way facilitate, any transactions with countries, companies, or individuals that are targeted under the respective EU, US or UK sanctions programme. Employees who are EU, US or UK persons are not requested or expected to provide guidance on transactions for any members of the Group where a risk of "facilitation" exists.
SAN4	**Comprehensive Sanctions** The Group considers the following countries and regions as being subject of a comprehensive sanctions programmes and applies relevant restrictions: Cuba, Iran, North Korea, Syria and the regions of Crimea and occupied territories in Ukraine and Georgia.

SAN5	**Screening Scope** All relevant parties, customers, stakeholders, transactions, deals, third parties and employees, are duly screened, including but not limited to customers, occasional customers, intermediate shareholding structures, beneficial owners, directors, authorised signers, powers of attorney, guarantors, business relationships, activities, transactions, occasional transactions, payments, deals, trade finance, providers, agents, intermediaries, employees and any other relevant third parties, as detailed in the related procedure. Incoming local transactions operated in Georgian Lari (GEL) via Real Time Gross Settlement (RTGS) are not subject to payment screening on the basis of the local regulatory expectations applicable on all banks to have their customers screened against UN, EU, US and UK sanctions regime.
SAN6	**Customer Timely Screening** Screening is done at on-boarding and on an ongoing basis. Anyone having a relationship with the Group is screened against applicable sanctions lists prior to the on-boarding. All changes and updates to the sanctioned lists or to the customer data is used as quickly as possible, and not later than 24 hours, for screening purposes throughout the course of the relationship.
SAN7	**Sanctions Risk Exposure** The Group ensures that an adequate customer assessment of the exposure to the sanctions risk is conducted at on-boarding and on an ongoing basis, which may be integrate into the AML/CTF Customer Risk Assessment. The Group, where appropriate, utilises both internal and reliable external sources to validate the customers' sanctions exposure.
SAN8	**Payment Screening Tool** The Group screens all applicable transactions, in real-time before the transaction is executed, against relevant sanctions lists. The Group defines and implements adequate screening tools, including fuzzy-logic, and assesses its effectiveness and efficiency regularly.
SAN9	**Trade Finance Screening** The Group makes sure all appropriate counterparty and transaction due diligence has been 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 programmes and/or restricted goods and trade regulations, including dual-use goods.
SAN10	**Employee and Relevant Third Party Screening** The Group does not recruit or hire employees or enter into or maintain relationships with relevant Third Party Service Providers, Landlords and Tenants, who are named on

	Sanctions Regulatory lists or who are permanently resident in a country under a comprehensive sanctions programme.
SAN11	**List Update** The Group establishes appropriate processes and procedures to review and refresh Sanctions lists on a regular basis.

SAN12	**Account Blocking** The Group establishes processes to block, freeze, reject or return financial transactions that are restricted or prohibited under applicable sanctions regimes, as well as transactions involving countries under a comprehensive programme and/or sanctioned entities or individuals to the extent required by applicable regulations. The Group reports to the relevant authorities if required and if applicable.
SAN13	**Circumvention** The Group defines, implements and assesses on an on-going basis with adequate control to prevent attempts of sanctions circumvention by customers, employees or any third party.
SAN14	**Sanctions Clause** The Group makes sure to include sanctions clauses in account opening, trade contracts and other transaction agreements when relevant to ensure compliance with this framework and associated policies and procedures.
SAN15	**Regulatory Reporting and Third Party Request** The Group 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 local regulations.
SAN16	**Reporting to the Sanctions Officer** The Group implements and maintains procedures and controls to ensure that any potential sanctions match or any transaction or series of transactions requiring a "Specific Licence" or subject to a "General Licence" is immediately escalated to the International Sanctions Unit within AML/ Sanctions Compliance Department.

Anti-Bribery and Corruption Statements

The following ABC statements are requirements applicable to level 2 ABC policies, including policies maintained by Procurement, Outsourcing and Human Resources departments.

AB&C Statements	
ABC1	**Compliance with ABC policy** The Group, its Supervisory and Executive Boards, employees, agents, contractors or any temporary employees does not engage in the facilitation of bribery and corruption, and does not aide or abate a customer or business counterparts to be involved in related activities, in Georgia or abroad.
ABC2	**Cash Payments, Political Contributions and Facilitation Payments** The Group, its Supervisory and Executive Boards, employees, agents, contractors or any temporary employees does not directly or indirectly offer, promise, give or authorise cash payments, political contributions or facilitation payments.

ABC3	**Gifts and Entertainments** The Group ensures that all permitted Gifts and Entertainment (G&E) 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 the Group, its employees, third

	parties or any other persons or entities, and are in compliance with the internal procedures, including records in the G&E Register.
ABC4	**Sponsorships, Donations, Charitable Contributions and Speaker Fees** The Group ensures that sponsorships, donations, charitable contributions and speaker fees are not to be offered, provided, or accepted in exchange for obtaining or retaining an improper advantage for the benefit of the Group, its employees, third parties or any other persons or entities.
ABC5	**Third Party Risk Assessment** The Group 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.
ABC6	**Hiring** The Group ensures that all offers of employment, whether permanent or temporary, are fair, transparent, merit-based and in line with Human Resource (HR) requirements, specifically in relation to candidates related to public officials.
ABC7	**Escalation to Compliance Unit** The Group 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 the Compliance Unit Head. The Group ensures that various means of escalation are available to the employees, including whistle blowing.
ABC8	**AML Investigation** The Group ensures that any suspicion of bribery or corruption, even if only an attempt, by a colleague, a customer, a business counterpart or any other third party, independently of the escalation to the head of Compliance Unit, is investigated by the Head of AML/Sanctions compliance department for potential filing with the FMS.

Policy Breach, Dispensation and Review Frequency

- **Policy Breach**

  The provisions of this Policy are mandatory. Any deviation from these provisions must be escalated to the Head of AML/ Sanctions Compliance Department immediately. A breach of this Policy may result in disciplinary action, up to and including dismissal and referrals to local law enforcement, in addition to the civil and criminal penalties for any of the parties involved.

- **Dispensations**

  It is not expected that exception or deviation to this Policy will be requested other than in very exceptional circumstances and with a strong rationale. Exceptions to the requirements of this Policy for specific customers, business partners, third parties, deals or transactions, provided it does not breach local AFC regulatory requirements, can be granted only by the joint approval of the Head of AML/Sanctions Compliance Department and the Chief Risk Officer and are reported to the Board for transparency.

- **Review Frequency**

  The Policy is a Supervisory Board level policy and is reviewed on an annual basis. However, this Policy may also be reviewed in situations where there is a relevant change in applicable legislation, regulation, or BasisBank's strategy, risk appetite or experience with incidents of AFC breaches.

Roles and Responsibilities

- **Supervisory Board**

  The Supervisory Board, or the relevant body at the Supervisory Board level, is responsible for setting and monitoring the risk appetite in respect to AFC, providing oversight of the AFC programme and approving the level 1 AFC Policy.

- **Executive Board (Board of Directors)**

  The Executive Board reviews and makes recommendation on the level 1 AFC Policy and on related frameworks in respect to managing the AFC risk in a proportionate and timely manner, is responsible for their implementation across the Group and for the oversight on the AFC risk management programme.

- **Head of AML**

  The Head of AML/Sanctions Compliance Department is responsible for the day-to-day implementation of the AML/CTF and International Sanctions programme, for the regulatory surveillance on AML/CTF and International Sanctions risks, for the completion of the AML/CTF and International Sanctions enterprise-wide business risk assessment, for the development of the AML/CTF and International Sanctions policies and procedures, for the day-to-day management of the controls under the direct responsibility of the AML//Sanctions Compliance department, for reporting of suspicious activity to the relevant authorities, for the development, implementation and maintenance of the monitoring and quality assurance testing to ensure effective compliance, for the development and delivery of AML/CTF and International Sanctions training, for the provision of advisory services to the first and second line of defence, and for reporting and escalation on AML/CTF and International Sanctions programme status and potential risks or breaches to the Chief Risk Officer.

- **Head of Compliance Unit**

  The Head of Compliance Unit is responsible for the day-to-day implementation of the ABC programme, for the development of the ABC policies and procedures, for the development, implementation and maintenance of the monitoring to ensure effective compliance, for the development and delivery of ABC training, for the provision of advisory services to the first and second line of defence, and for reporting and escalation on ABC programme status and potential risks or breaches to the Chief Risk Officer.

- **Deputy CEO, Risk Management**

  The Deputy CEO, Risk Management, is responsible for the managerial oversight on the AFC programme as developed, reported and escalated by the AML/Sanctions Compliance department and Compliance Unit. The Deputy CEO, Risk Management, is responsible for the reporting and escalation of AFC relevant topics to the Executive Board and Supervisory Board.

- **Employees**

  All employees are responsible for compliance with the requirements set out in this Policy. Any employee shall immediately contact the Head of AML/ Sanctions Compliance Department if there is any uncertainties with regards to this Policy and/or in cases of actual or suspected breach of this Policy.

- **Internal Audit**

  The Internal Audit, being the third line of defence of the Bank, is responsible for overseeing and auditing the work of the first and second lines of defence.

Control and Monitoring

- **Key Risk Indicators**

  The Group establishes appropriate KRI and monitoring measures to assess ongoing compliance as per the requirements set out within this Policy.

- **Monitoring Measures**

  The Group establishes quality assurance and testing measures to review AFC processes including over:
  - KYC data completeness and accuracy;
  - CDD at on-boarding and on-going maintenance;
  - Correspondent Relationships controls;
  - Transactions Monitoring review and FIU reporting process;
  - Monitoring and screening tools parametrisation and risk relevance;
  - Customer and payment screening alerts review;
  - Sanctions circumvention controls;
  - Enterprise wide business risk assessment and key risk indicators data quality assessment;
  - Board reporting and regulatory reporting data quality assessment; and
  - Anti-Bribery higher risk area assessment.

Appendix 1 – Acronyms

ABC	Anti-Bribery and Corruption
AML	Anti-Money Laundering
AML/CTF	Anti-Money Laundering / Combatting Terrorism Financing
BB	BasisBank
BB Group	BasisBank Group
CRA	Customer Risk Assessment
CDD	Customer Due Diligence
CTF	Counter-Terrorism Financing
EDD	Enhanced Due Diligence
EU	European Union
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FMS	Financial Monitoring Service of Georgia
HR	Human Resources
GEL	Georgian Lari
G&E	Gifts and Entertainment
GRECO	Group of States against Corruption
Group	BasisBank Group
KRI	Key Risk Indicators
KYC	Know Your Customer
ML/FT	Money Laundering / Financing of Terrorism
NBG	National Bank of Georgia
OFAC	Office of Foreign Assets Control

OFSI	Office of Financial Sanctions Implementation
PEP	Politically Exposed Person
RBA	Risk-Based Approach
RTGS	Real Time Gross Settlement
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
TM	Transaction Monitoring
UBO	Ultimate Beneficial Owner
UK	United Kingdom
UN	United Nations
US	United States of America

Appendix 2 – Glossary

Associated Person is a third-party individual or organisation that while providing products and/or services to the Group, interacts with other external parties.

Bribery is the offering, promising, giving, authorising, soliciting, agreeing to receive or accepting anything of value to/from another person or entity, either directly or indirectly to or by an individual, in order to improperly induce, influence, or reward the performance of a function or an activity.

Comprehensive Sanctions Programmes seek to prohibit most financial and commercial interaction with a specific territory or country or its government. Comprehensive Programmes generally prohibit (with few exceptions) all direct or indirect activity or facilitation with a territory or country, including imports, exports, and the provision of any financial products or services. Comprehensive Programmes may also include specific individuals or entities named on a sanctions list.

Corruption is the "trading in influence" and refers to any activity that involves the abuse of position or power for an improper personal or business advantage, whether in the public or private sector, and includes bribery.

Donation and Charitable Contribution is the voluntary giving of help to support those in need.

Employees are all the individuals working within the Group at all levels and grades, including senior management, officers, directors, employees (whether permanent, fixed term or temporarily), consultants, trainees, seconded staff, interns or any other person associated with the Group, wherever they are located.

Facilitation Payments (also called "facilitating", "speed" "expediting" "back-hander" or "grease" payments) is a form of bribery in which small payments are made with the purpose of expediting or facilitating the performance by a public official or a routine governmental action and not to obtain or retain business or any other undue advantage.

Licences and Exceptions on International Sanctions should be consulted on a regular basis. If a license is in place, certain individuals or/and entities might be allowed to engage in a certain conduct that would otherwise be prohibited by the respective sanctions regime. There are various licences available under US, EU, UN and UK regimes. The AML department will advise on sanctions licenses and procedures to follow.

List-Based Sanctions Programmes impose more targeted restrictions than Comprehensive or Selective Programmes. List-Based Programmes generally prohibit all activity with and require freezing or blocking of the assets of listed individuals and entities. List-Based Programmes can be either country-based or activity-based.

- Country-based programmes target listed individuals and entities associated with certain current or former governmental regimes that may threaten the stability of the country or region or commit large-scale human right abuses.
- Activity-based Sanctions Programmes seek to restrict all activity with listed individuals, entities, groups, and vessels that are deemed to be involved in activities such as terrorism, narcotics trafficking, transnational organised crime, and nuclear proliferation.

Outsourcing is an arrangement of any form between the Group and a service provider by which that service provider performs a process, a service or an activity that would otherwise be undertaken by the Group.

Public Officials are officials or employees of any government or other public body, agency, or legal entity at any level, including officers or employees of State-Owned Entities (SOE) and officers or employees of entities which are mandated by a public body or a state-owned entity to administrate public functions.

Sanctions Facilitation can mean any approval, referring business to a third party, acting for the benefit of a Sanctioned Party, financing, providing transportation, or insurance for transactions involving Sanctioned Parties.

Selective Sanctions Programmes seek to prohibit specific activity such as imports of certain goods or dealings in certain financial products with listed individuals and entities in a country or target activity involving certain industry sectors. Selective Programmes may also target current or former government bodies and current or former government officials including individuals and entities closely associated with the government.

Sponsorship is a commercial transaction that involves paying a fee in exchange for providing exploitable commercial opportunities associated with the agreed consideration.

Third Party is any external individual or organisation which provides products and services to the Group.

1 St. Queen Ketevan Ave., Tbilisi, Georgia
+995 322 922 922
info@basisbank.ge