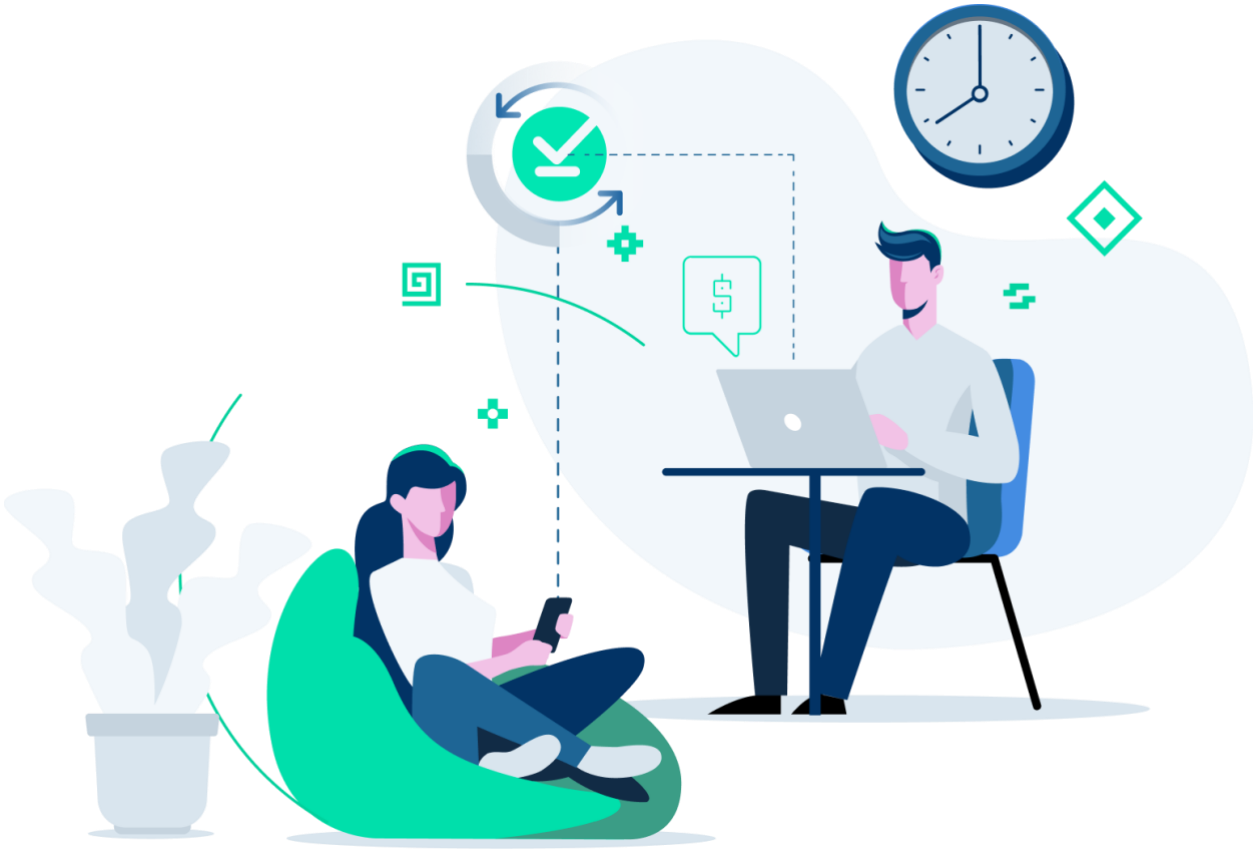
ANTI-MONEY LAUNDERING STANDARD

Standard

GGC-MA-0101-KU

Version 7

July 2023



Date	Developed by	Reviewed by		Approved by	Approver signature
26/07/2023	Head of Compliance Liliana Carvajal	Chief Governance & Compliance Officer Eduardo Cantón	DS EC	Executive President Sebastián Castro	DocuSigned by: 138A4B5AC97F4F7...
	Compliance Officer Fabián Durán			Chief Executive Officer Aron Schwarzkopf	DocuSigned by: Aron Schwarzkopf 0BC028A8CBC7426...
	Head of Corporate Governance Marisol Vera				

TABLE OF CONTENTS

Figures

Tables

1 INTRODUCTION

In response to the growing concern of the global community about the issue of asset laundering and terrorism financing, henceforth asset laundering and terrorism financing, Kushki's Senior Management is committed to its responsibility to prevent and combat them. Accordingly, it has adopted this document that brings together the policies and processes aimed at preventing and mitigating the consequences that these criminal behaviors may cause to the company.

2 LEGAL FRAMEWORK

Kushki and all its subsidiaries (hereinafter the “Company”, Kushki”, or the “Entity”) created its system to prevent asset laundering, terrorism financing, and proliferation of weapons of mass destruction based on the best international practices, as well as the recommendations by the Financial Action Task Force (FATF), the various UIF, and the local regulations applicable in each country where Kushki operates.

This standard lays out the corporate guidelines that apply to Kushki in the various countries where it operates or where it has openings. Likewise, on chapter 17 related documents, there is a list of documents that supplement the legal framework for each country.

3 SCOPE

This standard contains procedures, guidelines, and preventative measures against Asset Laundering (AL), Terrorism Financing (TF), Financing of the Weapons of Mass Destruction Proliferation (FWMDP), and other crimes leading to those. The scope of the current document is applicable to all products and services offered by the Company and its subsidiaries, as well as its clients, shareholders, providers, and employees. Likewise, it applies to physical and legal persons that have contractual relations with the company.

4 DEFINITIONS

Active business: a business establishment that holds transactions regardless of their frequency and amount.

AML (Money Laundering Prevention, which includes): AL/TF/FWMDP (Asset Laundering, Financing of Terrorism and Financing of the Weapons of Mass Destruction Proliferation). For all purposes of the implementation in each region where Kushki runs operations.

Bribery: means the behavior of a subject, which, actively or passively, is intended to give an employee or public official a compensation that falls outside that of his or her position.

Bribery: the crime of bribery is an active or passive behavior by a public servant, which purpose is to receive an undue payment taking advantage of his or her position, for himself / herself or for a third party.

Cash transaction: any cash transaction over ten thousand American dollars (U$10,000) or its equivalent in Chilean pesos (CLP) based on the dollar amount at the exchange rate applicable on the transaction date.

Client behavior profile: means all typical and habitual characteristics of the subject of analysis, concerning their general information and with the way they use the services and products offered by the entity.

Client: any natural person or legal entity with whom the payment processor establishes or holds a contractual relationship, in order to obtain the provision of a service, offered within the framework of the line of business or supplementary thereto, in accordance with the legal and/or regulatory framework, and said service provision may be of occasional, sporadic, unique, repeated, frequent or permanent nature.

Compliance Officer: means the official responsible for controlling that the management of the asset laundering and terrorism financing risk is compliant, by proposing that the residual risk is kept at appropriate levels, through the application of preventive policies, processes and procedures and the identification of unusual and unjustified transactions.

Correspondent: national or foreign financial entity with whom business or banking relations are held upon execution of an agreement.

Counterparty: is any natural person or legal entity with whom the Company holds trade, business, contractual or legal ties of any kind. Inter alia, the partners, employees, customers, contractors and suppliers of Company Products are deemed counterparties.

Customer transaction profile: is the parameter that indicates the maximum capacity that a client must transact with the entity. Its value or range is estimated using recognized technical methodologies considering variables such as its income, equity, economic activity, historical transactionality, inter alia.

Distribution channels: means used to provide financial products and services, namely - offices, automatic teller machines (ATM), point of sale terminals (POS), interactive voice response (IVR), call center, contact center, non-bank correspondents, remote access systems for customers (RAS), Internet, Mobile Banking, inter alia.

Enhanced Due Diligence (EDD): means the most demanding and reasonably designed set of policies, processes and procedures applied to internal and external clients, which, based on their greater exposure to risk and the cases described in the regulations, are applied by the entity to mitigate the asset laundering and terrorism financing risk.

Final beneficiary: means the natural persons who own or hold a client and/or natural person on whose behalf a transaction is carried out or who benefits from it, whether directly or indirectly. It also includes persons who hold ultimate effective control over a legal entity or legal agreement.

Financial Intelligence Unit (UIF): it means the technical unit responsible for collecting information, developing reports, implementing national policies and strategies for the prevention and eradication of asset laundering and terrorism financing.

Financial transaction: means an agreement or contract with the participation of two or more economic entities by exchanging capital, in such a way that the capital lender serves as a creditor, while the other serves as a borrower. Furthermore, the exchanged assets shall be equivalent at each given time.

High-risk activities: those activities which, due to their particular characteristics, entail a greater risk for the controlled entities of being used when committing ML and crime financing, including TF.

Inactive business: a business that does not carry out transactions for three months in a row.

Inherent risk: is the level of risk inherent to the activity, without considering the effect of the controls that have been put in place.

Jurisdiction: geographic location where an activity, operation or economic transaction is carried out.

Lead: natural person or legal entity who has requested information and expressed interest in receiving the services or products provided by the controlled entity.

Liable entities: are the economic sectors required to report and comply with the regulations for the prevention of asset laundering and terrorism financing and weapon of mass destruction proliferation, as specified in the local regulatory framework of each country.

Management elements for the prevention of asset laundering and terrorism financing (AML) risks: these are a set of components through which the administration of the asset laundering and terrorism financing risk, in controlled entities is implemented in an organized, systematic, and methodical fashion. These are the policies, organizational structure, manual and information, procedures, reports, audits, technology infrastructure, organizational culture and training aimed at mitigating the asset laundering and terrorism financing risk.

Market: means the set of people and/or organizations that take part in some way in the purchase and sale of goods and services or in the use thereof. To give a specific definition of market several variables are to be considered, such as the product, cycles, sales, jurisdictions, or a certain area.

Methodologies: it means the way in which each one of the procedures that the controlled entities use are defined and treated. It is the succession of logical, documented steps, linked together for a verifiable, operational, and reliable purpose, which, depending on their clients, products and services, channels and jurisdiction, inter alia, the controlled entities are to use to develop and evaluate the AML, by identifying clients and their risks, establishing transactional, behavior and risk profiles, applying processes to detect unusual events and managing reports.

Money laundering (ML): means an action carried out in any way intended to hide and/or disguise the illegal proceeds of certain goods, being aware that they come, directly or indirectly, from the perpetration of acts constituting crimes such as drug trafficking, terrorism, weapons, financial statement fraud, public fund embezzlement, treasury fraud and bribery, inter alia; or when being aware of said origin, hides and/or conceals these assets.

Money laundering and crime financing risk management, including terrorism (AML): set of actions adopted by the entity, in order to minimize the probability of a risk and/or its impact. The actions established for the Asset laundering and terrorism financing risk management program consist of mitigating and preventing the asset laundering and terrorism financing risk.

Monitoring and/or follow-up: means the continuous and systematic process through which the efficiency and effectiveness of a policy or process is verified, by identifying its strengths and weaknesses to recommend corrective measures aimed at optimizing the expected results.

Policies: means the guidelines, recommendations or aspects that support the prevention and monitor the asset laundering and terrorism financing risk.

Politically Exposed Persons (PEP): means national or foreign natural persons, who work or have worked as outstanding public servers in the country or abroad on behalf of the country, their relatives and related persons. (This category will be defined in accordance with the local regulations of each country where Kushki runs operations).

Products: these are financial mechanisms or instruments that, in accordance with the law, are provided by entities from the public and private financial sector.

Provider of strategic goods and services: natural person or legal entity that provides the products or services required for the financial entity to comply with critical processes related to its corporate purpose and which deficiency, weakness or suspension could affect the usual transactional development of the entity, with greater emphasis on the goods and services related to asset laundering and terrorism financing monitoring and prevention.

Related party: the related party is a natural person or legal entity, associated or linked to the entity controlled by property, administration or by suspicion, who has the possibility of exerting influence over it.

Related persons: includes those people who benefit from being close to the politically exposed person, such as their co-workers, advisers, consultants and personal associates.

Residual or net risk: resulting level of risk after controls have been applied.

Risk exposure: level of risk to which the entity is exposed before the events related to asset laundering and terrorism financing take place and is expressed through residual risk.

Risk factors: means the agents that create a risk or parameters that allow evaluating the particular circumstances of customers, products and services, channels and geographical location.

Risk management stages for the prevention of asset laundering and terrorism financing (AML): means the identification, measurement, control and monitoring of the asset laundering and terrorism financing risk.

Risk matrix: is a control and management tool that, through the identification and measurement of risk events related to the business lines and processes of the entity and to asset laundering and terrorism financing, allows the determination of the inherent risk and the implementation of the relevant due diligence monitoring and actions, from where the resulting residual risk is obtained.

Risk of asset laundering and terrorism financing and proliferation of weapons of mass destruction: is the possibility of loss or damage that a controlled entity may suffer due to its exposure to being used directly or through its transactions as an instrument for asset laundering and/or to channel funds to carry out criminal activities, including terrorism, or whenever they intend to conceal assets derived from said activities. This risk materializes through associated risks (legal, reputational, transactional and contagion) with the consequent negative economic effect that it may entail due to its financial stability when is used for said activities.

Risk profile: means the client risk condition both due to its behavior and transactionality that may expose the entity to events with asset laundering and terrorism financing implications.

Risks associated with asset laundering and terrorism financing: means the consequences for Kushki derived from the materialization of risks, such as:

- **Legal risk:** means the possibility that a controlled entity may suffer direct or indirect losses; that its assets are exposed to situations of greater vulnerability; that its liabilities and contingents may be increased beyond the expected levels, or that when conducting transactions it faces the possibility of being negatively affected due to error, negligence, inexperience, recklessness or fraud, derived from non-compliance, incorrect or untimely enforcement of legal or regulatory provisions as well as general or particular instructions issued by law-enforcement agencies, within their respective powers; or, in adverse jurisdictional or administrative rulings or resolutions, or due to the poor wording of the texts, formalization or execution of acts, contracts or transactions, including those other than those of their ordinary line of business, or in the event the rights of contracting parties have not been clearly established.
- **Reputational risk:** it is the possibility of affecting the prestige of a controlled entity by any event, external, internal failures made public, or by being involved in transactions or relationships with illicit businesses, which may lead to losses and cause a deterioration of the entity's prestige.
- **Transactional risk:** is the possibility of losses occurring in the controlled entities due to events arising from failures or errors in processes, by people, information technology and unexpected external events. It includes legal risk, but excludes systemic and reputational risks. It groups a variety of risks related to internal control deficiencies that affect the entity's ability to meet its commitments in a timely manner or compromise its stake.
- **Contagion risk:** it is the possibility of loss that an entity may suffer directly or indirectly, due to the action or experience of a third party.

Segmentation: process by means of which risk factors are classified into homogeneous groups internally and heterogeneous transversely. This classification is based on the recognition of significant differences in their characteristics.

Senior management: hierarchical level in the organization which decision-making process is autonomous. It is made up of the legal representatives, presidents and senior VPs, general managers, VPs or department managers and other professionals responsible for implementing the resolutions by the Board of Directors or the body acting on their behalf, in accordance with the assigned roles and the organizational structure defined in each institution.

Services: means all interactions of controlled entities with their customers and users.

Shell banks: those that do not have a physical branch in its country of incorporation which receives an operating license and is not part of a regulated financial group that is permanently subject to the supervision of the regulatory authorities. “Physical branch” means when there is a managerial and personnel structure in a country that allows the standard operation of the Bank. The mere existence of a local agent or low-level staff does not constitute a physical branch.

Shell company: means a duly incorporated Company, which does not carry out the established activities in its entirety or partially carries them out and which is used to cover up other activities.

Simplified Due Diligence: means the set of less demanding policies, processes and procedures, which empowers the controlled entity to apply them whenever it identifies a low-risk exposure to asset laundering and terrorism financing.

Supplier: means any public or private natural person or legal entity that develops production, manufacturing, importing, construction, and distribution activities.

Suspicious transaction: means a transaction that, due to its number, quantity or characteristics does not fit into the system and normal practices of the business, a given industry or sector. Furthermore, in accordance with the uses and customs related to the activity in question, it cannot be reasonably justified.

Suspicious Transactions Reporting (STR): it does not entail a complaint, but it consists only of useful and relevant information so that the FIU or UAF may employ financial intelligence and, thus, identify signs suggesting ML and/or TF.

Terrorist financing: abbreviated as TF is any form of economic action, assistance or mediation that provides financial support to the activities of terrorist associations or groups. Although the main objective of terrorist groups is not financial, they require funds to carry out their activities, which may come from legitimate sources, criminal activities, or bot.

Transaction: financial action that formalizes the transaction held between the debtor and creditor through payments or money by means monetary instruments.

Transfer: means the transaction carried out by a natural person or legal entity called the payer, through an entity authorized in the relevant jurisdiction, to carry out transactions to wire national and/or international funds, so that a sum of money is made available to a natural person or legal entity called the beneficiary, through the same institution or another one that may be authorized to conduct this type of transaction.

Unusual and unjustified economic transaction: financial actions carried out by natural persons or legal entities that do not match to the transactional and behavioral profile established by the entity and which cannot be supported or whenever, even though these may be consistent with the customer's line of business and profile, they seem excessive and unusual due to their amount, frequency, or recipients.

Unusual transaction: means a transaction which amount or particular characteristics are not related to the economic activity of the client(s) that carry it out, or that, due to its frequency or the traded amount, falls outside the normal parameters established for a given market, or whenever its reasonableness or justification are questionable.

User: means the natural person or legal entity who, without being a client of the controlled entity, receives a service thereof.

Warning signs: mean the Client’s behavior or the characteristics of certain financial transactions or otherwise that in their national or international experience suggest suspicious transactions or asset laundering and terrorism financing typologies and could lead us to timely and/or prospectively identify the possible existence of a asset laundering and terrorism financing risk.

5 ORGANIZATIONAL STRUCTURE

Kushki has established the following structure for the integration of the different areas of work in the enforcement of AML policies and procedures.

Figure 5.1
Organizational structure

6 ROLES AND RESPONSIBILITIES

6.1 Duties of the Board of Directors

The Board of Directors shall be responsible for:

- Approving the AML manual as well as its amendments from time to time.
- Appointing a collaborator as Compliance Officer, to be responsible for ensuring the implementation, monitoring, and verification of compliance with the prevention of asset laundering and financing of crime, such as terrorism, in the countries and among the business groups where the company has a footprint.
- Approve the reports submitted by the Chief Risk Officer / Head of Risk & Compliance on the results of the evaluation and analysis of the program efficiency and effectiveness, along with the improvement proposals that may be applicable.
- Determining the transactional, economic, physical, technological, and resource measures that may be required for the Compliance Officers to perform their duties in each country where the company has operations and in every associated entity.
- Approving the training program to prevent asset laundering and financing of crime, such as terrorism.
- Approving the methodologies, models, qualitative and quantitative indicators, matrices and more instruments or tools to prevent the risk of asset laundering and financing of crime, such as terrorism.

- Providing efficient and timely support to the Compliance Officer by having access to all processes and information that said officer may request.
- Imposing within the scope of its responsibility and subject to due process and in accordance with the law, the internal penalties ordered by those who fail to comply with the provisions herein.

6.2 Duties of the Chief Risk Officer / Head of Risk & Compliance

- Oversee the strict compliance with all the regulations associated with the prevention of asset laundering as provided in laws, regulations, standards, handbooks, and guidelines applicable at the regional level.
- Report to the Board of Directors about all matters associated with compliance, including, from actions linked to the development and monitoring of policies and to the application of penalties for non-compliance.

6.3 Duties of the Chief Governance & Compliance Officer (CCO)

- Ensuring the implementation of policies regarding (AML) at a regional level.
- Ensuring that the company has a risk management policy in place.
- Establishing a culture within the organization that emphasizes its commitment to internal controls, risk management, and high ethical standards.
- Ensuring that appropriate channels for reporting compliance issues are in place.
- Measuring and evaluating the level of compliance with all regulatory requirements throughout the organization.
- Reporting on all matters related to Compliance from development and monitoring of policies to the application of penalties for non-compliance to the Board of Directors

6.4 Duties of the Compliance Officer or his or her alternate in case of absence

The Compliance Officer is at the managerial level with decision-making powers concerning everything that involves the implementation for the prevention and control of asset laundering and terrorism financing; accordingly, he or she shall be responsible for:

- Monitoring strict compliance with all provisions related to the prevention of asset laundering in laws, regulations, standards, manuals, and instructions.
- Submitting quarterly reports on the results of the evaluation and analysis of the program efficiency and effectiveness, along with the improvement proposals that may be applicable.
- Preparing the AML Manual and submitting it for approval, and to propose the relevant updates and ensure its dissemination to employees.
- Permanently monitoring compliance with the Know Your Customer policies, by orchestrating and checking due diligence processes through the implementation of the procedures, mechanisms, and methodologies herein.
- Evaluating the reports submitted by the internal audit or whoever performs similar functions or acts in their stead, and the reports submitted by the tax auditor or the external audit, if applicable, and adopting reasonable actions when facing any reported deficiencies. If the actions to be adopted require authorization from other bodies, he or she shall advocate for these matters to be brought to the attention of the relevant bodies.

- Checking compliance with the due diligence and enhanced due diligence procedures applicable to the Company.
- Carrying out the evaluation of the ML/TF/FWMDP risk to which the Company may be exposed.
- Informing the CCO about possible failures or negligence in the controls established to mitigate the identified risk situations that may compromise the employees' and Kushki's responsibility.
- Managing the AML stages and elements in order to prevent the asset laundering and terrorism financing risk and identify unusual and unjustified transactions, by determining the risk and proposing mitigation actions.
- Establishing and disseminating the classification criteria of clients, based on their level of risk.
- Developing, along with the risk area, the specific procedures, methodologies, models, qualitative and quantitative indicators, matrices and more instruments to manage the asset laundering and terrorism financing risk for the approval of the Legal Representative.
- Reporting to the Financial Intelligence Unit of each country, or to the entity that takes its place, the reports as an obligated entity, including, but not limited to, any Suspicious Transaction that comes to their attention, by accompanying the background information that may be required for its proper review.
- Certifying before third parties whenever it is required by a processor, purchaser, Bank, the existence of the system for the prevention of asset laundering and terrorism financing.
- Addressing and orchestrating any requirement, request or diligence of court or administrative authority responsible for the prevention and control of criminal activities.
- Addressing queries from internal and external clients on matters of prevention of asset laundering and terrorism financing.
- Orchestrating both the transaction follow-up activities as well as the investigations that shall be carried out at the institutional level concerning asset laundering and terrorism financing.
- Timely adopting corrective actions against the observations issued by the internal and external audits, the Superintendencies or control and surveillance bodies of each country.
- Orchestrating and designing the annual awareness and onboarding training program for all employees. Likewise, timely communication matters related to training, in coordination with Human Resources to the CCO.
- Adopting the appropriate actions to keep the documents related to the prevention of asset laundering and terrorism financing, in a confidential and secure manner, in accordance with the procedures established in the legal provisions.

6.4.1 Limitations and Restrictions of the Compliance Officer or his or her alternate in case of absence

- Being part of control bodies or areas directly related to the activities established as part of the main corporate purpose.
- Being an outsourced employee of the entity.

6.5 Duties of the Head of Transactional Monitoring

- Draft the process for the compliance transactional monitoring and management at a regional level.
- Manage (identify, analyze, escalate, among others) the transactions that display warning signs associated to ML/TF situations.
- Automate the transactional monitoring process by implementing tools and models based on machine learning and artificial intelligence.
- Keeping the transactional monitoring system updated so that it can identify, manage, and document, in real time, the warning signs and all unusual and/or suspicious transactions (transactions that do not match the client's business activities or surpass the established parameters) through an automated analysis.
- Support the risk identification, measuring, control, and monitoring processes for AML and compliance at a regional level.
- Support the analysis process applied on clients deemed to pose higher risks.
- Support the processes linked to ALP and other projects from the Compliance area.
- Create a segmentation of risk factors as defined by each entity.

6.5.1 Duties of the Compliance Specialist

- Support to the Compliance Officer in the implementation of methodologies, models, qualitative and quantitative indicators, matrices and more instruments to manage the risk of asset laundering and financing of crimes, such as terrorism.
- Draft the documentation related to the different processes and procedures for the proper management of the asset laundering and terrorism financing risks.
- To provide support in the development of internal training programs for employees, suppliers, and business establishments.
- Overall, all the duties inherent to this position or those that may be assigned by the Compliance Officer.

6.6 Duties of the Auxiliary of Transactional Monitoring

- Support the processes to identify, measure, manage, and monitor risks associated with AML and compliance at a regional level.
- Support the implementation of various projects at a regional level.
- Perform the analysis of alerts generated by the transactional monitoring application.
- Support the segmentation of risk factors based on the individual level of risk of each client.
- Analyze and manage alerts in the international restrictive lists (FATF, OFAC, UN, among others).

6.7 Duties of the Internal or External Audit

- To conduct an annual evaluation of the Asset Laundering and Terrorism Financing Prevention program, in order to verify the effectiveness of the existing controls in place in accordance with the defined work plan.

6.8 Duties of the Internal Compliance Committee

- Evaluate unusual operations reported by the Head of Monitoring to assess the relevant report to be filed to the various UIF at the regulated countries.
- Make a monthly review of the alerts generated in the transactional monitoring tool based on a selected sample.
- To permanently monitor each of the stages and elements of the system, especially the risk matrix, emphasizing the actions taken to mitigate the entity's risk.

7 AML POLICIES

Kushki provides online payment services, which key pillar is to guarantee the security of transactions carried out through its technological platform. Hand in hand with this service promise, the company is committed to mitigating the risk that monetary transactions with proceeds of crime or which purpose is to finance criminal acts related to asset laundering and terrorism financing, are conducted through its platform. Therefore, there should be zero tolerance for this risk. Accordingly, it shall internally foster the open rejection of any criminal activity.

Furthermore, the company has defined the following internal policies for this purpose:

- Kushki is committed to adopting the local legal regulatory framework and good international practices, based on the transactions' size and complexity and the analysis of the level of inherent risk.
- Kushki does not provide services to businesses, suppliers, shareholders, final beneficiaries (individuals or legal entities), who are included in OFAC, UN, EUROPEAN UNION lists. Matches in other lists or negative public information related to asset laundering and terrorism financing, shall be considered an important criterion to deny or terminate a contractual relationship.
- Kushki, in compliance with its service terms and conditions, reserves the right to block, cancel and/or disable the transactional operation of any of its clients if unusual transactions are identified and for which no reasonable justification has been given.
- Kushki does not accept the inclusion of a business that has not filled out the digital form in its entirety by attaching the required documents for their affiliation.
- Kushki undertakes to carry out an adequate selection process of suppliers and employees with whom it is to establish a legal or contractual relationship to conduct its business.
- Kushki conducts business with natural persons and legal entities who develop legal activities. By identifying industries or items that, due to the nature of their business activities, could be considered as risky and with a greater probability in the materialization of asset laundering and terrorism financing and weapons of mass destruction proliferation and any predicate offense.
- Kushki establishes mechanisms to identify and confirm the information provided by third parties (customers, suppliers, employees, inter alia). In order to determine if these are listed as direct PEPs or related persons up to a 2nd degree of blood ties, by establishing the protocols required across the different countries where we run operations.
- Kushki does not establish business relationships with people who cannot prove the lawfulness of their income with which they acquire the products or services.

- Kushki does not establish business relationships with clients who perform transactions arising from political campaigns and/or political parties.
- Kushki shall report suspicious transactions, identified at any stage of the relationship flow to the relevant authorities by providing all the support and assistance required by said authorities as dictated by the law in force.
- Kushki fosters an asset laundering and terrorism financing culture, for which it shall maintain permanent disclosure and training plans.
- Kushki makes sure that its employees are aware of the content of this manual, its policies, procedures and their amendments from time to time to be protected from these risks. Likewise, Kushki's employees shall prioritize compliance with the regulations on asset laundering and terrorism financing risk management and observe ethical principles to achieve business goals.
- Kushki established a methodology to identify the risk factors and resulting asset laundering and terrorism financing-related events. Preventive detection or corrective controls shall be designed. Likewise monitoring activities shall be established to ensure that controls are comprehensive and work in a timely, effectively, and efficiently.
- Kushki does not carry out transactions to and from Countries that have not taken appropriate actions to mitigate the asset laundering and terrorism financing risk, and which are identified by international organizations, such as FATF, as high risk.
- Kushki digitally preserves the documents supporting the implementation of Asset laundering and terrorism financing.
- Kushki shall cooperate when authorized and/or required by the laws, authorities, supervisors, government, court, and law-enforcement agencies in the investigation of situations that may involve illicit activities, overall, but especially those related to asset laundering and terrorism financing or bribery.
- Kushki has a new product release procedure in place where potential risks are evaluated by establishing the appropriate controls.
- Through the Compliance Officer, Kushki shall immediately report to the different Financial Information and Analysis units or whoever acts in their stead in each country, in the event any good, Asset, Product, Fund or right of interest under the name or the administration or control of any country, person or entity included in blacklists Lists is identified or confirmed.
- Kushki shall not hold into business relations with Clients that are related to shell banks or direct relations with these banks or with institutions that allow their accounts to be used by them.

8 ML/TF RISK ASSESSMENT METHODOLOGY

Kushki’s methodology for the risk implementation and management is based on the ISO 31000 Risk Management standard, which provides a generic guide for the development of the Kushki’s asset laundering and terrorism financing risk management process at a regional level.

This document contains the methodology established by Kushki for ML/TF risk management, which involves the establishment of the internal and external context, the identification of risks, evaluation of inherent risk probability and impact, residual risk impact and monitoring the asset laundering and terrorism financing risk as well as the establishment of treatment plans, as appropriat.

8.1 Objectives

8.1.1 General objective

To evaluate the asset laundering and terrorism financing risk management system across the Company's different processes, considering the development of the program elements and stages in place to manage the asset laundering and terrorism financing risk.

8.1.2 Specific objectives

- To prevent Kushki from being used as an instrument for asset laundering or terrorist financing.
- To mitigate the risk of regulatory non-compliance related to the prevention of money laundering and terrorist financing (ML/TF).
- To prevent links of any kind with natural persons or legal entities found in the UN, OFAC, FATF, Al-Qaeda, etc. blacklists.
- To develop follow-up and continuous monitoring processes that allow the timely identification of suspicious or unusual transactions.
- To maintain the good corporate image of Kushki, an ethically correct company that has always been concerned about good practices and ML/TF prevention.

8.2 Reference framework

For the integration of the asset laundering and terrorism financing risk management process into the entity's processes, the following aspects are considered:

- Processes that may be vulnerable to the ML/TF risk or processes related to the asset laundering and terrorism financing risk management program are identified.
- Meetings are held with the employees responsible for the processes subject to evaluation and the Compliance department to build a work team to apply the methodology.
- Inherent risk events and their causes are identified as well as the risk and associated factors, which are evaluated based on the risk measurement process.
- The controls that mitigate identified risks are classified and evaluated. Those controls that are no longer applied are removed, as appropriate, and/or mitigation controls are proposed, based on the control qualification process.
- The process residual risk is estimated.

8.3 Risk management process

8.3.1 Background

To define the basic parameters for risks to be managed and to provide decision-making guidance when conducting more detailed risk management evaluations, the entity's background or context is to be established.

8.3.2 External context

- Regulatory framework on asset laundering and terrorism financing risk.
- Current regulations applicable to the business in accordance with the local recommendations of each country where Kushki runs operations.

- Other external entities:
  - FATF recommendations.
  - Types of asset laundering and terrorism financing published by the relevant FIU or UAF.

Other factors that impact on the external context are the political and geographical scenario, economic sectors, domestic or international outlook, which may impact on the entity's processes on ML/TF, e.g., entering a new market, a new product, service channel or jurisdiction.

The work team shall consider compliance with the current regulations on money laundering and terrorism financing risk as well as the identification of new typologies for risk assessment in the process.

8.3.3 Internal context

Kushki is a company with experience in the payment method sector, which provides its affiliates with the possibility of accepting payments worldwide and receiving money in their local currency. It connects different payment methods in each country into a single integration. Understanding the importance of each business, it always seeks to adapt the service according to the client's needs, creating world-class payment experiences.

Increasing the effectiveness of payment processes and, thus, providing a simple and seamless payment process. Allowing the easy handling of all payment methods - credit and debit cards, bank transfers and cash, in one place.

The entity has a qualified work team who is highly committed to great customer service, backed by a highly efficient transactional and technological platform. Its business model is part of risk management systems, auditing processes by always seeking to streamline it.

Regulatory framework

The asset laundering and terrorism financing risk management Program Manual for each jurisdiction shall be complied with, as well as with the code of ethics, government code, anti-fraud and anti-corruption policies, and other policies that may be established by the Company.

The work team shall consider the current internal regulations on asset laundering and terrorism financing Risk, based on the evaluated process. In other words, the procedural standard of the processes to be evaluated, which are published in the process tool, is to be referred.

8.4 Identifying the asset laundering and terrorism financing risk

- The risk identification process shall be permanent and answer the questions: what could happen, how and why events or situations that affect the fulfillment of the entity's objectives due to its exposure to the asset laundering and terrorism financing risk may arise, for which purpose the questionnaire used to identify ML/TF risks may be used as a reference.
- In the risk identification stage, all risk factors shall be considered and a list of possible events that may lead to an asset laundering and terrorism financing risk that may affect Kushki's fulfillment of ML/TF objectives shall be created.

- The techniques used to apply methodology in this stage a restructured interviews with process experts, whose evaluation is carried out using a questionnaire to identify ML/TF risk.
- Using the existing sources of information on events that could generate risks for the entity. These sources include:
  - Suspicious Transactions Reporting (STR) by the entity.
  - Typologies developed by financial intelligence units.
  - Red flags published by FATF.
  - Press information
  - The opinion of the entity's expert responsible for the process.
  - Risk factor segmentation.
- Accordingly, the possible scenarios that may expose the entity to ML/TF risks are defined below:
  - Arise from a customer relation.
  - Arise due to non-compliance with standards.
  - Being related to the entity's income.
  - Being related to the income destination by the business or user.
  - Being related to the entity's good standing.
  - Being related to the entity's operation in sanctioned countries.
- Once the risks have been defined, these shall be related to the following risk factors defined by the relevant entity for each region:
  - Clients
  - Products
  - Channels
  - Jurisdiction
- The Compliance Specialist, along with the person responsible for the process or the employees designated by the same shall be responsible for the identification of ML/TF risks, and their associated risks, as well as the risk factors, so as to identify the causes that lead or that could lead to the materialization of the risk and that are ultimately listed in the risk matrix, in accordance with the procedure described in the asset laundering and terrorism financing risk management program manual.
- For an approximation to the process reality when it comes to risk identification, the scenarios below shall NOT be deemed risks:
  - Risk-related causes
  - No controls in place
  - Control not working
  - The expected loss or impact of an event
  - The opposite of the goal defined in the process
- Lastly, in outsourced processes or where outsourcing is involved, the risk shall be identified and assessed by the process Leader or those who serve as supervisors of a third party.

8.5 Measuring or evaluating the inherent risk of money laundering and terrorism financing

Once the risk identification stage is completed, the probability of occurrence of the inherent risk (with no controls in place) is measured against each of the risk factors, considering the frequency and/or probability criteria of the risk occurrence and the extent of impact if it were to materialize.

8.5.1 Evaluating the probability of occurrence

It is a qualitative and/or quantitative approach that describes whether a risk situation is likely to occur or not. This may be measured by the occurrence possibility of an asset laundering and terrorism financing event. Considering factors that may lead to risk, even if it has not occurred in the past.

The scale used by Kushki to measure the probability of occurrence in terms of frequency is as detailed in Table 8.1 below.

Table 8.1
Probability measure

FRECUENCY			
Classification	**Level**	**Description**	
Very high	5	The event occurs in over 25% of the transactions.	The number of exposure events is over 25 times a year.
High	4	The event happens in 15% to 25% of the annual transactions.	The number of exposure events is a maximum of 25 times a year.
Medium	3	The event occurs in 5% to 15% of the annual transactions.	The number of exposure events is a maximum of 15 times a year.
Low	2	The event occurs in 2% to 5% of the annual transactions.	The number of exposure events is a maximum of 5 times a year.
Very low	1	The event occurs in in 2% of the annual transactions.	The number of exposure events is a maximum of 2 times a year.

8.5.2 Estimating the impact scope

It refers to the consequences or results that would occur in the event the asset laundering and terrorism financing risk were to materialize. For impact assessment purposes, the impact classification table was established and consists of a scale of five (5) levels determined in Table 8.2 below.

Table 8.2
Impact measurement

Level	Legal	Reputational	Transactional	Contagion
VERY HIGH	Losses due to administrative penalties over 0.5% of the company's equity.	The reputational consequences are known by the public. Impact that harms the entity's image due to unsafe practices that result in loss of trust, intervention and penalties. Reputational consequences at a regional level.	Flaws in processes, resources, infrastructure, technology or non-compliance with internal regulations with a serious impact that causes damage that result in operating costs that affect the entity's assets.	The event is considered serious due to the participation of the related party in ML that compromise the entity.

Level	Legal	Reputational	Transactional	Contagion
HIGH	Losses due to administrative penalties of less than 0.5% and over 0.36% of the company's equity.	The reputational consequences are known by the financial sector, processors and other related parties, failure disclosure and/or investigation by the regulatory body. Impact that affects the entity's image due to insecure practices.	Flaws in processes, resources, infrastructure, technology or non-compliance with regulations or internal regulations with a significant impact that causes damage, resulting in a higher operating cost.	The risk event involves the participation of a person linked by an employment or contractual relationship with the entity that may be involved in ML/FT.
MODERATE	Losses due to minor administrative penalties of less than 0.36% of the company's equity.	The reputational consequences are known by the senior management and control bodies. Reputational consequences at a national level.	Flaws in processes, resources, infrastructure, technology or non-compliance with regulations or internal regulations with a moderate impact on the development of management processes.	The risk event involves the participation of a person linked to the entity that may affect its economic and administrative situation.
LOW	No economic impact. The risk occurrence does not result in a cost or penalty caused by non-compliance with regulations.	The reputational consequences do not go beyond the entity. No reputational damage caused to the entity; the situation is known by the senior management.	Flaws in processes, resources, infrastructure, technology with minor impact and that do not affect management processes.	The contagion possibility for the entity is lower. There are no significant correlations that affect the entity's relation with the market, customers or related parties.
VERY LOW	No economic impact. The risk occurrence does not result in a cost or penalty caused by non-compliance with regulations	No external impact. The image and good standing of the entity are not affected.	Flaws in the processes due to the restructuring the entity's human or technological resources.	Other related parties involved in ML that do not have collateral effects that may harm the entity.

Identified risks shall be related to an associated risk (reputational, legal, transactional or contagion), considering the impact that it may generate if it were to materialize.

Based on the impact classification table and associated risk, the risk impact if it were to materialize is established.

8.5.3 Assessing the related risk level

After determining the probability and the inherent impact for each risk cause, the inherent profile (with no controls in place) is estimated, measured according to the impact criteria probability, and is pinpointed on the entity's risk map.

The risk level is determined as a numerical value, which is obtained as the result of the values assigned to the occurrence probability and impact, in the event associated risks materialize.

Inherent Risk = Associated Value Frequency x Associated Value Impact

Inherent risk profile scale

For this purpose, a scale divided into 4 ranks, see Table 8.3.

Table 8.3
Inherent risk scale

Level	Classification
1 - 4.99	LOW

Level	Classification
5 - 9.99	TOLERABLE
10 - 14.99	SEVERE
15 - 25	CRITICAL

8.6 Building the risk map

- In accordance with the entity's guidelines on risk management, Kushki develops risk maps, taking the COSO ERM (Enterprise Risk Management) methodology as a reference framework, in order to apply international standards to the entity's risk management.
- For Kushki, risk maps constitute an effective tool to graphically identify the risk events with higher exposure, which allows prioritizing based on their urgency level, facing any vulnerability that requires timely decision-making.
- Money laundering and terrorism financing risks are plotted in the following risk model to make their management easier.
  - The result of the probability and impact combination determines the level of inherent risk or exposure to ML/TF risk of the identified risk.
  - The risk level is determined as a numerical value, which is obtained as a result of the concatenation of the values assigned to the occurrence impact and probability in case of materialization of the associated risks.
  - As a result of the foregoing, the risk levels established by Kushki are defined as per the following risk severity quantification matrix.
  - With the result of the inherent level of each one of the causes, the consolidated risk map is developed by process, and the entity's consolidated process where the exposure of risk events with no controls in place is observed.

Table 8.4
Heat map

		IMPACT				
		Very low	Low	Moderate	High	Very high
PROBABILITY	Very high	0	0	0	0	0
	High	0	0	0	0	0
	Medium	0	0	0	0	0
	Low	0	0	0	0	0
	Very low	0	0	0	0	0

8.7 Money laundering and terrorist financing risk control

It is the set of actions adopted by the entity to minimize the probability of the materialization of a risk and/or its impact. The actions established for the Asset laundering and terrorism financing

risk management program consist of mitigating and preventing the asset laundering and terrorism financing risk.

In this stage, the controls are identified and evaluated to determine their effectiveness on the identified risks, which purpose is to minimize the risk probability or impact in the event it materializes.

The criteria defined to evaluate the effectiveness of the controls in place to mitigate the asset laundering and terrorism financing risk are described below.

8.7.1 Monitoring evaluation criteria

Monitoring classification and evaluation is determined through the four (4) essential monitoring attributes below: OPPORTUNITY, AUTOMATION, APPLICATION, and IMPLEMENTATION. Each of them has been assigned a maximum weight of 25 out of 100 points as detailed on Table 8.5 below.

Table 8.5
Monitoring Classification

Variable	Criterion	Value	CONCEPT	Max Score
Opportunity	Preventive	25	This monitoring control prevents the occurrence of risk	25
	Detectional	15	This monitoring control identifies the materialization of a risk	
	Corrective	5	This monitoring control corrects the impact of a risk occurrence	
	Non-existent	0	There is no control associated to the risk occurrence	
Automation	Automated	25	This monitoring control runs automatically by the software	25
	Combined	15	This monitoring control runs in the system with a manual component	
	Manual	5	This monitoring control is run purely by a human resource	
	Non-existent	0	There is no control associated to the risk occurrence	
Application	Permanent	25	This monitoring control is applied permanently and certain periods	25
	Periodic	15	This monitoring control is applied when needed only	
	Occasional	5	This monitoring control is applied at times at the owner's responsible	
	Non-existent	0	There is no control related to a risk occurrence	
Implementation	Total	25	This monitoring control is documented, disclosed, and incorporated into the process	25
	Partial	15	This monitoring control is in place, but not documented and the other way around	
	None	5	This monitoring control is not documented, disclosed, or incorporated into the process	
	Non-existent	0	There is no control related to the risk occurrence	

- Opportunity: it refers to the time when a control is run when conducting an activity.
- Automation: it refers to the degree of control systematization at the time of its application intended to minimize its manual operation.
- Application: it refers to the frequency with which a control is applied, in order to mitigate the materialization of a risk.
- Implementation: it refers to the degree of formality and disclosure of the control within the company's document system.

Subsequently, the sum of these rating criteria yields the maximum score of each control by risk cause. Which, depending on how its weighed, it may be ranked based on the following scale to determine its rating and the individual mitigation effect it has on each cause:

Table 8.6
Rating and mitigation effect

Rank	Rating	Mitigation effect
90 to 100	HIGH	75%
65 to 89	GOOD	55%
35 to 64	STANDARD	40%
11 to 34	MODERATE	25%
1 to 10	INSUFFICIENT	10%
0	NON-EXISTENT	0%

Lastly, the individual mitigation effects are weighted to obtain the average mitigation of each risk-related controls. This percentage shows the effectiveness of the control in mitigating the risk impact and frequency, which, once applied to the inherent risk, allows obtaining the residual risk assessment.

8.8 Residual risk assessment

8.8.1 Residual risk profile

The residual risk profile is the consolidated result of the measurement of the risks to which Kushki is exposed, where the following formula is used to calculate the risk profile:

RP = X (R (R/ ZA)) i.e.: **RP** = (a x (a/R)) + (b x (b/R)) +... (n x (n/R))

RP: Risk profile

a: Risk 1

b: Risk 2

n: Risk n

R: Sum of risk levels (a + b +...n)

The formula allows determining a consolidated risk profile, considering the risk profile represented by the percentage of each of its individual risks. The result of this calculation follows the simple rounding method.

8.8.2 ML/FT risk acceptance level

Kushki's Board of Directors has defined that its maximum residual risk acceptance level within the ranking is Low, i.e., the exposure result considering the effect of the controls on the identified inherent risks.

8.8.3 Managing residual risk

Once the control action against the inherent risk has been evaluated, the final assessment result shall be included in the Table 8.7 according to its criticality, so as to define how the residual risk is to be managed.

Table 8.7
Residual risk classification

Level	Classification	Description
1 - 4.99	LOW	With this risk level, periodic monitoring shall be carried out to ensure control compliance.
5 - 9.99	TOLERABLE	When risk falls within this level, action plans and/or specific controls are required to handle it.
10 - 14.99	SEVERE	For this level, controls must be strengthened or short-term action plans must be defined; furthermore, the Risk Committee shall be informed for follow-up.
15 - 25	CRITICAL	In this case, the Risk Committee shall intervene directly and immediately inform the company's Board of Directors.

The residual risks classified as LOW and TOLERABLE shall be evaluated annually by the Process Leaders with the support of Compliance, so as to ensure control effectiveness over time, either by improving it or defining new controls when required. If a risk level increase is perceived, this shall be reported immediately to the SRCC Committee (Security, Risk and Compliance Committee) so that the relevant reclassification is conducted.

For residual risks classified as SERIOUS or CRITICAL, the Process Leader shall establish action plans aimed at reducing the company's exposure by creating new controls or implementing modifications to existing controls.

These plans shall be monitored on a quarterly basis, and their progress shall be reported to the SRCC Committee (Security, Risk and Compliance Committee) and the Board of Directors, for them to make the relevant decisions for to handling and mitigation. The actions adopted by Kushki to mitigate or treat residual risks are as follows:

- **Risk elimination:** an administrative decision is made to suspend the product or process.
- **Risk mitigation:** material internal changes shall be made to processes due to control improvement, activity redesign or elimination, aimed at reducing the impact or frequency distribution, or both.
- **Risk dispersion or scattering:** It is achieved by distributing or locating the risk in various places, processes or people.
- **Risk transfer:** it seeks support and/or to share the risk with a counterparty.
- **Risk assumption:** after a risk has been minimized or transferred, a residual risk may remain. In this case, the Board of Directors accepts the tolerable residual loss and shall define specific treatments to manage these risks.

8.9 Monitoring an asset laundering and terrorism financing risk

Monitoring seeks to evaluate the evolution of the entity's risk, both inherent and residual, and its variation as well as the control effectiveness in order to determine the corrective actions that may be required.

8.9.1 Monitoring Kushki Management

- The purpose of monitoring ML/TF risk management in the company's areas or processes is to track the inherent and residual risk profiles, and the stages of the asset laundering and terrorism financing risk management program in order to take the corrective, preventive and system improvement actions.
- The individual and consolidated evolution of risk profiles, risk factors and adopted controls as well as the related risks shall be carried out every six months.
- Likewise, a follow-up audit to the several units evaluates controls in accordance with the follow-up work plan designed for the Company’s asset laundering and terrorism financing risk management program.

9 RISK FACTOR SEGMENTATION

Kushki's methodology to segment by risk factors is based on the CRISP-DM methodology, which stands for Cross-Industry Standard Process for Data Mining, and it is a proven method to guide data mining jobs, as per the following phases:

- Business understanding
- Data understanding
- Initial data collection
- Data description
- Data exploration
- QA checking
- Data preparation
- Modeling
- Evaluation
- Deployment

Kushki, with a tool of recognized statistical value, determines the characteristics of typical transactions and compares them with those carried out by the clients, in order to identify Unusual and/or Suspicious transactions in a timely manner.

9.1 Kushki risk factors

In accordance with our business model, when offering, selling and supplying our products and services, we face the following four (4) different risk factors that expose us, to a greater or lesser extent, to the ML/FT risk:

- Our Counterparties
- Our products
- The channels

- Jurisdictions

To identify Kushki's asset laundering and terrorism financing risk, each risk factor must be understood. For this and according to the tool obtained by Kushki, they are grouped based on the homogeneous characteristics of each risk factor.

10 PROCEDURES

10.1 Know your counterparty procedure

10.1.1 Know your business procedure

This pillar includes the proper identification of the clients to whom Kushki is to provide its payment service. The business or establishment that intends to use our technological products shall fill out an affiliation form available on our website and upload the required documentation.

Once the affiliation forms available on the website have been completed, a series of steps that are to be completed by several Kushki business areas will be triggered before the customer can start operating with the service.

The first activity of the affiliation process consists of validating the risk profile. This process is intended to get to know the customer in depth by searching in restricted, national, and international control lists through the designated tools, including their credit profile. To generate an acceptance criterion based on the results of the business searches, a decision matrix is used. This, as a result of many weightings so as to allow setting a minimum acceptance limit for the business in the Gateway model affiliation, if a match is found in the searches, in accordance with our policies, the client's enrollment shall not proceed, in which case, the process would be suspended.

All this due diligence, found in more detailed in the process, is intended to prevent the products or services provided by Kushki from being used as instruments to conceal, manage, invest or divert money or other assets which origin or destination are the proceeds of crime. For this reason, the business channels are required to get to know the clients, as this is structurally key to prevent the asset laundering and terrorism financing risk.

Within the due diligence framework, the following actions aimed at getting to know the customer shall be taken:

- Identifying the Client and verifying its identity through the documents issued by the authorities of each country for said purpose.
- Identifying the final beneficiary of businesses, for Kushki to know who they are.
- Understanding and, when appropriate, obtaining information on the purpose and nature of the business relationship.

For the purposes of mitigating the legal and reputational risk of having relationships with natural persons and legal entities included in OFAC, UN, EUROPEAN UNION, and local lists thereafter, the system continuously monitors natural persons and legal entities.

Kushki conducts a data updating process based on the risk level of each active business, and inactive businesses will be updated when they no longer have such condition.

As part of this pillar, some risky and prohibited businesses are considered, as shown in the document **GGC-IN-0104-KU** Mapping risky and forbidden businesses. It must be noted that businesses considered riskier should go through the Compliance area for review and understanding. During this analysis, the area will request additional information and documentation as necessary to convey the policies or measures adopted to prevent asset laundering and financing of crime, such as terrorism.

10.1.2 Know your employee procedure

- For the recruitment, selection and hiring process, the documents described in the Recruitment and Selection process of the Human Resources department shall be managed and requested from participating candidates.
- Before performing a job, Human Resources shall properly learn information on the candidate and other rules defined for this purpose and shall also search the candidate in restricted lists through the internal application provided by the Compliance area to prevent ML/TF risks. The result from this list search, the candidate's resume, security profile (when applicable) and other documents required during the selection process, shall be filed in the employee's file.
- Searching restricted lists shall be carried out after an inclusion to check that there is no change in the information and that they have not been reported in any restricted list, therefore, Compliance shall run a validation every year on all active employees of the company, and search evidence thereof is to be included in a folder under its custody.
- In the event a report is positive, the Compliance Officer in each country where the company has operations shall be informed immediately via email to the address compliance@kushki.com / compliance@billpoket.com.
- The personal data of the company's active employees is updated annually.

10.1.3 Know your supplier procedure

Hand in hand with the company's values, we are committed to working solely and exclusively with suppliers and/or partners that are aligned with Kushki's principles. There are key guidelines for the selection and evaluation of suppliers of goods and services that Kushki may require that are applicable to all local and foreign suppliers of goods and services that seek to work with Kushki and any of its subsidiaries and which service directly impacts on Kushki’s service provision.

- To select a specific supplier, the relevant evaluation shall be carried out based on criteria specified in the supplier selection and evaluation procedure.
- Kushki shall query beforehand the information of the provider in the Restricted Lists/Blacklists before engaging.
- Kushki shall REFRAIN from working with suppliers (individuals or legal entities) with criminal, court, credit, tax records or obligations and/or who are included in blacklists or restricted lists.
- The query in the restricted lists shall be carried out after the enggement to validate that there are no changes in the information and that they have not been reported to any of the restricted list. Therefore, the Compliance area shall carry out a yearly validation of all the active providers at the Company, leaving evidence of the query in the shared folder for Compliance.
- Kushki shall cancel any contractual relationship if there is evidence that a provider is included whether in a national or international blacklist and restricted list related to asset laundering and terrorism financing.

- Kushki reserves the right to block, cancel and/or disable the service relationship with any third-party provider if it fails to comply with the contractual provisions.
- Kushki shall request an annual update from recurring suppliers through the mechanisms provided for this purpose.

10.1.4 Know your shareholder procedure

- In no case Kushki fails to identify and learn the basic information of all of its shareholders, including the final natural persons or effective beneficiaries of a legal entity.
- Annually, Kushki checks that shareholders are not included in blacklists, restricted lists, including the condition of PEP persons. In the event of coincidences, the relevant actions shall be taken.

10.1.5 Final beneficiary

In order to comply with the local regulations and based on international standards such as the FATF, Kushki has implemented several mechanisms to record the information of the final beneficiaries of affiliated businesses, including an express statement by the business when filling their information on the virtual form or in the form **GGC-FO-0107-KU** Statement of final beneficiary form, which includes fields to register the partners or shareholders of each company in the regulated countries, which is part of the Kushki Affiliation process.

10.2 Procedures for politically exposed persons

The Compliance Officer shall use the databases provided by the list provider to identify PEPs.

As for those clients who have been identified in this category, the relationship shall be approved by the higher authority from Sales applicable in the regions where Kushki has operations. In general, the actions established in the procedure **GGC-PD-0103-KU** Enhanced Due Diligence shall be taken.

Monitor the transactions of PEP clients from time to time in order to determine whether they are within normal parameters or not when compared against the profile of their segment.

From time to time, Compliance shall review the client database in order to determine if any of them have acquired a PEP status after their affiliation process.

10.3 Procedures for natural persons and legal entities that have a current relationship with kushki and are included in restricted lists, blacklisted or in other watchlists or news

Once the continuous monitoring process finds a natural person or legal entity in a blacklists list or subject to a tax process in local lists, the contractual relationship shall be terminated in accordance with the provisions of the terms and conditions, and the Compliance Official shall report this to the relevant Intelligence Unit, and to the transactions area to remove the client, then, the business unit shall report this situation back to the client.

That the Compliance Officer, in its monitoring process, finds relevant news on natural persons or legal entities with whom a contractual relationship is established, thus, he or she shall report this to the Legal Representative, how this situation is to be treated, depending on the Reputational or Legal Risk this may represent for Kushki, they may be asked to explain the situation and, thus, take the relevant actions.

10.4 Business transaction monitoring procedure

Hand in hand with the Know Your Customer process, Kushki manages the transactional monitoring process for asset laundering and terrorism financing risk through the information recorded on business transactions in the Monitoring Dashboard and based on which alerts were defined considering the behavior, nature and characteristics of each business. Alerts are generated based on statistical settings and are further reviewed by the compliance specialist. In the event an atypical behavior is identified, the business area is notified, which, in turn, shall issue a warning as per the due diligence process and subsequently notify Compliance, who shall determine the closing of the unusual transaction.

To determine whether a transaction is suspicious, it shall be submitted to the internal Compliance committee, along with the analysis supporting information and according to the applicable business unit warning, where the STR shall be determined. Subjective criteria shall not be taken into consideration, the analysis shall be duly supported and documented.

10.5 Procedure to determine or use alert signals

These are the facts, situations, events, amounts or financial indicators that fall outside the particular characteristics of clients or markets, from which the possible existence of a fact or situation that falls outside the ordinary course of Kushki business may be identified.

The following warning signs are general notions and take those provided by the UAF or by the national authorities on their websites as guidelines. These guidelines are based on the actions and situations associated with Kushki's activities as well as its relations with clients and the information obtained from them. Every Kushki employee is under the obligation to immediately report any situation they deem worthy of reporting identified during their ordinary activities to the Compliance Officer through Slack, the whistleblower channel, or the following email addresses compliance@kushki.com / compliance@billpocket.com, including the following:

- Whenever the client provides insufficient or inconsistent information and shall argue that it is to be supplemented or clarified in the next few days.
- Whenever customer transactions are not consistent with their economic activities and their transactional profile.
- Whenever the client refuses to provide information that allows confirming their income streams.
- Whenever customers show little knowledge about their business.
- Whenever the documents submitted by the client are questionable concerning their business existence.
- Whenever they show reluctance or annoyance when asked to fill out the affiliation forms or to clarify the data therein.
- Whenever an employee has a lifestyle that does not match their income.
- Whenever an employee is reluctant to take vacations, to accept changes in their activity or promotions that implies that he or she will not continue to carry out the same activities.
- Whenever the client gives an address that matches the address of another business that differs from the one that was declared or does not fit the declared line of business

- Whenever the client carries out transactions in high amounts and does not declare a paid job or activity that justifies the amounts involved.
- Customers which postal address and account statements is abroad or match a post office box.
- Unusual and unjustified increase in the billing of a client's business, observed from the economic activity recorded in their accounts and profile.
- A client that in a short period appears as the owner of new businesses or companies, incorporated with significant startup capital.
- A client who carries out repeated transactions on behalf of third parties.
- A client who frequently sends or receives money transfers to or from countries considered non-cooperative by the Financial Action Task Force (FATF), or territories listed by the Organization for Economic Co-Operation and Development (OECD) as preferential tax regimes, without an apparent economic justification.
- Incorporation of companies with capital or partners from non-cooperative jurisdictions by FATF or damaging preferential tax regimes according to the OECD classification (Tax Havens).
- Sudden change in the ownership of a company, which new partners show a business profile that does not match the entity's history, or who may be reluctant to submit personal or financial information.
- A client who refuses or suspends a transaction when required to provide information on the origin of certain funds.
- Opening of multiple businesses with a person in common to all of them.
- Clients whose companies have people who do not match their position profile as directors.
- Clients whose companies show a non-operating income higher than the operating income at the time of registration and/or when making an update.
- Clients whose financial statements show results that are not consistent with the industry or sector average.
- If a client is being investigated or prosecuted for asset laundering and terrorism financing or predicate offenses becomes publicly known in the media or otherwise.
- Transfers requested by a client to several people with no apparent relationship.
- Transfers sent to different countries under the same beneficiary and within a short period.
- Transfers made to several people who share common information (address, telephone, inter alia) are identified.
- Funds are received from various senders, who share common information (address, telephone, inter alia) are identified.
- Large amounts sent via online payment processing companies (PayPal, Money bookers, etc.) which do not provide information about the sender are received.
- Clients who carry out transactions in jurisdictions that are not related to the corporate purpose to the usual jurisdiction.
- Companies that have a very low capital and/or a very broad corporate purpose.
- Clients that change their bank accounts and/or their final beneficiaries on very short periods of time.

- Existence of one or more business accounts through which a large number of transfers are made to and from abroad, and for which there does not seem to be a sufficiently justified business or economic purpose, particularly when this activity is carried out from or to countries, territories or jurisdictions subject to special monitoring (countries designated by national authorities, or countries and territories designated as non-cooperative by the FATF or the OECD).
- Use of virtual transfer links between traditional bank accounts and anonymous payment services (Money Services Business, virtual currencies, digital currency exchangers or alternative payment channels such as e-cash, e-wallet), in order to stratify the funds from the original source and collect them into one or more accounts via transfers to or from places of concern.
- Creation and operation of non-governmental organizations (NGOs) or non-profit organizations (NPOs) which activity or corporate purpose is not justified by the characteristics of the area or place where it holds operations, the frequent reception and sending of money to or from abroad, the unjustified use of funds in relation to the purpose for which it was created, non-existence of the required infrastructure to conduct its activities, receiving cash contributions to fund its internal operations, or being linked to external persons who receive or forward money to third parties.
- Non-profit organizations (NPOs) that base their existence on receiving contributions from countries considered to be of high terrorist risk.
- A transaction does not match the profile of a customer or counterparty businesses, or the end user information does not match their business profile.
- A client or counterparty declared a business activity whereby it carries out transactions that suggest that it may be acting as a money transfer business or as a payment account. These accounts involve fast high-volume transactions and a small balance at the end of the day for no clear business reasons. In some cases, the activity related to payers seems to be related to entities that may be associated with a state-sponsored proliferation program (such as shell companies operating near countries with proliferation or diversion concerns), and the beneficiaries seem be associated with manufacturers or shippers subject to export controls.
- Stake in a small business, brokerage/intermediary business that may be conducting activities that are inconsistent with its usual business.
- The transaction pattern of a client or its counterparty, which claims to be a business, suggests that it is acting as a money remittance company.

10.6 New product procedures

Whenever a new product is designed and before it is launched to the public, the Compliance department shall carry out an assessment of the asset laundering and terrorism financing risk to which this product may be exposed and establish the appropriate controls to mitigate these risks for each case.

Each product technical sheet shall be submitted to the Compliance department for assessment and determine whether each product has the appropriate controls in place; otherwise, the area responsible for implementing and putting them in place shall be required to do so.

10.7 Due diligence actions[1]

Given the risk profile of each Client, Kushki may apply one or more of the following actions, which are applicable to all countries, including Chile:

- **For high risk profiles** the enhanced due diligence actions under the procedure **GGC-PD-0103-KU** Enhanced due diligence must be taken. All potential clients who fall into any of the following categories shall be directed through Kiss Flow to the Compliance area:
  - National and Foreign PEPs.
  - Non-governmental organizations (NGOs) or charities
  - Clients who carry out cross-border business transactions with high-risk countries where Kushki does not run operations.
  - Risky and restricted businesses (**GGC-IN-0104-KU**).
  - Customers with unusual transactions found by Compliance.
  - Clients with Negative Background.
- The simplified due diligence actions may be applied (optionally) to **low-risk profiles**:
  - Fill in the simplified due diligence data by using third-party data sources.
  - Postponement of the obligation to check the client's and final beneficiary's identification information when an act and/or transaction is carried out above a certain monetary threshold.
  - Customer identification data is updated with less frequency.
    - Enhanced Due Diligence (DDI) data based on information obtained from third-party sources is updated.
    - The client's Continuous DDI is less thorough. This lower degree of thoroughness may be dependent on a monetary threshold.
    - Waiver from the request for information on the purpose of the legal or contractual relationship, or of the occasional transaction.

Notwithstanding the foregoing, the Simplified Due Diligence actions shall not be applicable whenever there are ML/TF suspicions concerning a client.

11 TRAINING PROGRAM

The training objective shall be to disseminate, promote and foster a culture of prevention of asset laundering and terrorism financing for the protection of both employees and the company.

The training is mandatory for employees in the onboarding course. The program is updated once a year and may be given online and/or in a classroom.

During this process the training program shall be focused on understanding the operation of the asset laundering and terrorism financing activities as well as its different stages, modalities and typologies related to the economic activity of Kushki. Likewise, emphasis is placed on the importance of warning signs, internal administrative and external criminal penalties, reinforcing

[1] Please refer to Procedure GRC-PD-AML-003-001 "Enhanced Due Diligence Procedure", to learn the details of this activity.

the content of this ML/TF prevention manual, the procedure to be executed when facing a suspicious transaction and internal reporting or complaint mechanisms. At all times, the confidentiality and anonymity of the whistleblower shall be protected at all times.

Furthermore, through Kushki's internal communication media (via Slack, or e-mail), newsletters, videos, news, blogs will be sent including topics and updates related to the prevention of asset laundering and terrorism financing.

In the ongoing course and every year after updating it, employees shall enroll in the Kushki Academy, where the ML/TF program is developed. Human Resources shall be responsible for keeping the monitoring and attendance indicators.

On the other hand, as a mechanism to determine the effectiveness of the training given to employees, the eLearning platform shall include a learning evaluation consisting of 5 questions, the test approval percentage shall be 80%. Those employees who obtain a grade lower than this percentage of approval shall receive feedback and shall re-take the test with a 100% acceptance approval.

Kushki trains third parties according to their nature. To this end, the company shall verify attendance and implement mechanisms to evaluate their performance. It is the company's responsibility to demonstrate these efforts.

12 DOCUMENTATION AND DISCLOSURE

This standard, and its associated documents, must be deposited in the document management tool. The Processes area will be in charge of disseminating the relevant updates.

Additionally, the documents below are listed:

- Minutes stating the approval of the manual designed for the prevention of asset laundering and terrorism financing.
- The documents and records supporting the design, development, and implementation of methodologies for the prevention of asset laundering and terrorism financing.
- The documents supporting unusual and suspicious transactions.
- The quarterly reports issued by the Compliance Officer.
- All additional documentation supporting the implementation and update of the program.

Kushki shall keep, in accordance with the conditions established in local regulations, the following documents for ten (10) years at least, unless the local laws of each country or the Kushki policy on document retention specify a longer period:

- Affiliated businesses link forms, where applicable
- Reports filed before the government authorities on suspicious customer activity related to possible asset laundering or other criminal conduct, along with the supporting documentation of said suspicions.
- Records of courses given on asset laundering including the names, levels and business units of the participants as well as the dates and places where the training was given.

- The due diligence and knowing your client record shall contain the information that the Clients deliver through the affiliation process and shall specify whether said Client is high or low risk for the purposes of taking Enhanced Due Diligence actions.
- Record of transactions carried out by Politically Exposed Persons (PEPs) shall contain the information related to any transaction carried out by any person who matches the definition of a Politically Exposed Person.
- Any other document that is to be kept as per the applicable asset laundering prevention laws in each country.

13 REPORTS

A key component of Kushki's Program to Prevent Asset Laundering and Terrorism Financing is making regulatory reports in the countries where the law thus require. Therefore, all employees, officers and directors are responsible for timely and appropriately reporting any non-compliance or unusual transactions they are aware of through the official channels provided by the company.

In addition, they shall be responsible for timely and appropriately reporting of any perceived issue or deficiency found in the policies, procedures, practices, or systems that may lead to non-compliances with Kushki policies or legal provisions.

13.1 Whistleblowing channel

Kushki has whistleblowing channels that guarantee anonimity, making it easier to report suspicious situations in which an employee, supplier, client, and/or third parties could involve the company, either directly or indirectly. The whistleblowers can choose any of the following alternatives to file their reports.

13.1.1 By email

The first option is by writing to the following email address lineaetica@kushkipagos.com. In the email subject, the reporting party must specify what is the behavior it wishes to report. In the text, the reporting party must describe, in detail, the events that took place. It is important to include the following information:

- Who carried out the action.
- Area and position of the person associated with the reported behavior (if the whistleblower does not know this information, include any other information that could help identify the offending party).
- Dates when the events took place. If possible, also specify the approximate time when they happened.
- If there is any evidence, please attach it to the email.
- If the event merits providing more background information, the Compliance Officer will contact the reporting party after filing the report. At all times, there will be guarantees of confidentiality and anonymity for the whistleblower.

13.1.2 Online

The second channel to file reports is by following this link: https://www.kushki.com/gobcorp/. In this portal, it is possible to file the relevant report by following a number of steps that the page will guide the user through in an intuitive manner.

Figure 13.1
Reporting online

13.2 Responsability

The responsibility for ensuring that reports on matters related to asset laundering and terrorism financing are developed and submitted rests with the Head or Director of Senior Management, area, or unit. By carefully following the rules and instructions outlined in this Manual along with the policies and procedures detailed in other manuals and transactions documentation, employees shall be protected from civil and criminal liability whenever a transaction is reported to the regulatory authorities.

Reporting is intended to:

- Keep the Board of Directors informed about significant issues and risks.
- Keep the Compliance area aware of the issues caused by asset laundering and terrorism financing activities, for them to adopt the appropriate corrective actions, as required.
- Focus attention and foster discipline and continued compliance with Kushki's regulations to prevent asset laundering and terrorism financing.
- Comply with the regulatory provisions to report unusual activities (e.g., suspicion of asset laundering or financing of terrorist activities).

13.3 Suspicious Operations Report (ROS)

Kushki is responsible for reporting to the Financial Intelligence units any operations it deems suspicious, following the local regulations applicable to each country.

13.4 Internal reports

All Kushki employees are required to issue the internal reports below:

- Internal Report on unusual transactions: through the channels enabled for this purpose. (Slack, e-mail compliance@kushki.com and/or the hotline).
- Internal report on suspicious transactions.

- Reports of the monitoring stage: as a result of monitoring activities, the compliance specialist shall develop a monthly report on this subject.
- Monthly Compliance Reports: the compliance officer shall submit a monthly management report to the Chief Governance & Compliance Officer.
- Quarterly report to the Board of Directors.
- Annual Management Report to the general shareholders' meeting.

13.5 Information confidentiality

All the information on Clients and transactions that Kushki keeps on their databases or records shall be strictly confidential. In this way, Kushki will ensure that the officials who have access to this information are only those who, due to their position, have the required permissions to have access thereto.

Kushki, its employees, partners and managers shall refrain from informing the affected party or third parties of whether information has been requested or submitted to the Financial Analysis Unit and providing any other related information.

14 TECHNOLOGY INFRASTRUCTURE

Kushki will ensure that the areas involved in the process of managing the risk of asset laundering and financing of crimes, such as terrorism, have the necessary technological tools so as to ensure strict compliance with the provisions in this handbook.

15 CONSEQUENCES OF NON-COMPLIANCE

Failure to comply with the policies, processes and controls established in this manual and, overall, the regulations related to the prevention of risks associated with asset laundering and financing of crime, such as terrorism, may result in penalties as indicated in **GRH-CO-0101-KU** Code of ethics and behavior, applicable to all employees, partners or third parties who fail to comply with them when carrying out their functions in the entity.

Some consequences derived from non-compliance with the processes established in this area are detailed below:

- Criminal penalties, fines, and custodial sentences in accordance with the provisions of the criminal code and current laws applicable in each country where Kushki runs operations, applicable both to natural persons and legal entities, when they fail to perform their legal obligations to prevent asset laundering and terrorism financing.
- Labor penalties, which may result in the termination of the employment contract, if it is proven, after conducting the relevant investigation, that the employee committed any of the following non-compliances:
    - Failure to comply with the policies and processes outlined herein or the code of ethics and conduct.
    - Disclosing the administrative or court procedures that may be brought against them to the business.
    - Disregarding any requests by the relevant authorities.
    - Allowing the concealment of proceeds of crime.

16 REFERENCES

- GGC-PL-0401-KU Policy for corporate risk management

17 RELATED DOCUMENTS

- GRH-CO-0101-KU Code of ethics and behavior
- GGC-PD-0103-KU Enhanced due diligence
- GGC-IN-0104-KU Mapping of risky and forbidden businesses
- GGC-FO-0107-KU Final beneficiary statement form
- GGC-DG-0102-CO PLA regional Colombia
- GGC-DG-0103-EC PLA regional Ecuador
- GGC-DG-0104-CL PLA regional Chile
- GGC-DG-0105-PE PLA regional Peru
- GGC-DG-0106-MX PLA regional Mexico
- GGC-DG-0107-BR PLA regional Brazil

18 CHANGE TRACKING

Version	Date	Changes made
V4	16/02/2021	*Adjustments in compliance with the Chilean regulations on Anti-Money Laundering and Terrorist Financing (AML/FT). *Adjustments made based on the recommendations given by the BDO External Audit.
V5	20/12/2021	3. Updated the DDC procedure code. 10.1.5. Specified the considerations about final beneficiaries in Chile and Colombia. 10.5. Indicated that the alert signs are taken as a guideline for what is specified by the UAF. 13.1. Added the chapter about whistleblowing channels at Kushki. 13.3. Expanded the second paragraph regarding requirements in Chile. 13.4. Added the steps to rectify a ROE. 16. Updated the list of reference documents.
V6	02/06/2022	2. Expanded the regulatory framework for all of Kushki's subsidiaries. Weapons of mass destruction were added to the PLA system. It is also specified that the system is also based on recommendations by the UIFs. Eliminated the table with regulatory frameworks by country. 3. Expanded the scope to all of Kushki's subsidiaries. 4. Eliminated the concept of DDC, Head of Crime Prevention, countries with a preferential fiscal regime, ROE, and UAF. Updated the definition of asset laundering and suspicious operations. 5. Modified Figure 5.1. 6. Updated the roles and responsibilities for the Board of Directors, CCO, Compliance Officer, Compliance Specialist, and Internal Compliance Committee. Added the roles of the Chief Risk Officer/Head Risk & Compliance, Chief of Transactional Monitoring, Auxiliary of Transactional Monitoring, and Internal Compliance Committee. Eliminated the functions of the legal representative, Head of Crime Prevention, Fiscal Auditor, and the requirements for the Compliance Officer. 7. Specified that Kushki does not engage in commercial relations with clients that carry out transactions associated with political campaigns and/or political parties.

Version	Date	Changes made
		8.8.3. Updated the name of the Risks Committee to SRCC Committee. 10.1.2. Updated the periodicity of consultations with contributors to the lists, from bi-annually to annually. Added the email address for Bill pocket. 10.1.3. Specified that the consultations to the lists of providers must be done before and after engaging. 10.1.4. Updated the periodicity of consultations of shareholders in lists, from bi-annually to annually. 10.1.5. Updated the procedure for final beneficiaries. 10.2. Approvals of PEP will be provided by the higher authority at Sales. 10.3. Indicated that KAM and the Support area could also communicate with the client about cancellation of services. 10.5. Added the email for whistleblowing and one instance to report unusual particular situations. Added as a sign for alert in bank accounts set for short periods of time. 10. Eliminated the chapter about procedures to record client transactions applicable to Chile. 11. Added training for third parties. 12. Document management is the responsibility of the Processes area. 13.1. Specified that the whistleblowing channels guarantees anonymity. 13.3. Updated the report of suspicious operations. 15. Eliminated penalties applicable in Chile.