Procedure for Risk Management.

DATE	VERSION
December 2022	First version

1. OBJECTIVE AND SCOPE.

This procedure defines the methodologies used for the different Stages carried out within the framework of the development and implementation of the Self-Control and Integral Risk Management System for Money Laundering, Financing of Terrorism, and Financing of the Proliferation of Weapons of Mass Destruction - SAGRILAFT. Therefore, a procedure is established for the identification, analysis, and management of risks in the processes, in order to bring them to an acceptable risk level, and thus favor decision-making and compliance with organizational objectives.

The content of this document is applicable in all processes of CCLA COLOMBIA S.A.S. (hereinafter "CCLA" or "Company"), begins with the identification, analysis, evaluation, treatment, and monitoring of risks and ends with the implementation, follow-up, and evaluation of plans to mitigate them.

2. DEFINITIONS.

For all purposes related to this Procedure, the terms listed below must be understood in accordance with the following meaning. The terms defined in the SAGRILAFT Compliance Policy are also part of this Procedure.

i. Risk Management: It is the description of the control measures that must be adopted to prevent, retain, transfer or modify the risk in the event of a possible materialization.

ii. Qualitative analysis: Is the description of the magnitude of potential consequences, the likelihood of those consequences occurring, and the associated level of risk.

iii. Risk Analysis: It is to establish the probability of occurrence of risks and their impact. Risk analysis depends on the information obtained in the Risk Identification phase.

iv. Risk Appetite: It is a high-level weighting of how much risk the Company is willing to accept in achieving its goals.

v. Risk Assumption: The residual risk that remains after the risk has been reduced or transferred.

vi. Risk Cause: The condition that gives rise to a risky event and causes uncertainty.

vii. Risk Sharing or Risk Transfer: Reduces its effect through the transfer of losses to other processes.

viii. Consequences: It is the set of effects derived from the occurrence of a situation identified as risky expressed qualitatively or quantitatively, whether losses, damages, disadvantages or gains.

ix. Corrective Control: They correct the negative effects of undesired events.

x. Detective Control: It is an alarm that is triggered in the face of an abnormal situation and as such they notify the appropriate people after an undesired event. They are effective when detection occurs before material damage occurs.

xi. Preventive Control: They deter the occurrence of undesired events. These are applied to the cause of the risk and its generating agent, in order to reduce the possibility of occurrence. It is the control that par excellence must be applied to prevent the ML/TF/FPWMD risk.

xii. Stages: It refers to the set of successive stages called risk identification, measurement, control, and monitoring.

xiii. Risk Source: Element that alone or in combination, has the intrinsic potential to originate a risk.

xiv. Risk Management: They are the coordinated activities to direct and control an organization with respect to risk.

xv. Egmont Group: It is an international body that brings together the world's Financial Intelligence Units (FIU) that facilitates the exchange of information to combat ML/TF/FPWMD.

xvi. Risk Identification: It is the description of the risks associated with a certain process.

xvii. Impact: It is the effect produced by the materialization of the risk in the objectives of the process.

xviii. DELPHI Methodology (Theodore J. Gordon and Olaf Helmer): A creative technique known as the Delphi Method seeks to bring together a number of experts and through discussion, to reach a common consensus.

xix. Probability: It is the possibility that potential sources of risk will actually materialize.

xx. Risk Management Procedure: It is this document.

xxi. Risk: It is the effect of uncertainty on the objectives.

xxii. Risk Severity: It is the qualitative value that arises from combining the variables' probability and impact.

xxiii. Risk Tolerance: It is the acceptable level of variation in relation to the award of an objective.

3. STAGES.

3.1. RISK IDENTIFICATION.

The purpose of this stage is to identify the risks that may arise when CCLA develops its activity. In order to identify the risks, the DELPHI methodology (Helmer & Gordon) will be used, which is based on the concept of experts both in the risks managed and in the Company's processes and procedures.

For which it will be necessary to form a panel of experts, which will be selected from key officials of each of the departments of CCLA, which must be contextualized by the Compliance Officer's team in terms of risks to be managed. Similarly, both internal and external information should be available, as described below:

Internal Information:

- Internal databases.
- Expert opinion of the Compliance Officer team.
- Opinion of selected experts from each CCLA department.

External Information:

- 100 cases of the Egmont Group, this is a compilation of high-profile anti-money laundering cases by Egmont Group member FIUs.
- Typologies and red flags documents published by UIAF - Colombia.
- GAFILAT Regional Typologies Report.
- GAFISUD – FATF typology report, refers to complex money laundering techniques.
- Press information.

3.1.1. EXPERT METHOD / EXPERT PANEL / DELPHI METHOD.

For all methodologies that include the participation of experts, the DELPHI method will be used, according to the following instructions:

a) Creation of an expert panel: Those responsible for each process shall select a group of persons with sufficient experience in the development of each process, to compose the expert panel in conjunction with the Compliance Officer's work team.

b) Methodology for construction and risk drafting: The expert panel from each department shall meet with the Compliance Officer's team, the latter having to contextualize to all attendees how the work methodology will be, for which they shall:

   i. Anonymously, each expert shall contribute according to their knowledge, with possible risks that they consider may affect the process or the Company.
   ii. The possible risks anonymously contributed will be discussed with all the attendees and unified in the event that similar typologies are contributed, likewise, the process of item (i) shall be performed again in the event that the attendees want to contribute more risks.
   iii. In conjunction with the expert panel and the Compliance Officer's team, the typologies that apply to the process in which the risks are being identified shall be selected; likewise, the Compliance Officer's team will be responsible for socializing possible risks that apply based on external information and/or their experience.

c) Technical documentation of risks: For the documentation of the risks identified based on the expert panel's knowledge, the following key elements of each risk should be considered in conjunction:

   i. No.: It is the code that allows differentiating each risk event from the others.
   ii. Risk Source Identification: It is that which has the intrinsic potential to do harm or generate opportunities.
      - Risk syntax or wording: Corresponds to the wording of risk for its understanding, taking into account its components.
      - Typology: Brief description of the risk that may arise in the development of the CCLA process or procedure.

iii. Why it may occur: It is the technical description of the causes, which usually directly or underlyingly allow the occurrence of the hazard source.
iv. When the risk occurs: It is associated with the source sub-process, which is most exposed or affected in the identified typology.
v. Where it may occur: Identifies the process directly related to the typology.
vi. How the risk occurs: Relationship of the risk with the typologies and warning signals that impact its occurrence.
vii. Risk Factor.

3.1.2. RECORDING OF THE IDENTIFICATION STAGE

Once the risks have been identified and the necessary technical information has been obtained, they will be approved by the Compliance Officer and subsequently included in the Risk Matrix.

It is important to point out that the risks identified at this stage and included in the matrix must be reviewed and updated by the Compliance Officer in conjunction with the departments involved on an annual basis, which is why when an employee identifies an imminent risk, he/she ought to notify the Compliance Officer for analysis, inclusion in the matrix and respective treatment.

The Risk Matrix defined is composed of the following fields, which will have the possibility of evaluating the risks individually and collectively:

No.	(WHAT)		(WHERE AND WHEN)	(HOW AND WHY)	RISK FACTOR
	TYPOLOGY	RISK EVENT	PROCESS AND/OR ASSOCIATED SUB-PROCESS	CAUSE OF RISK	

3.2. MEASUREMENT STAGE

The purpose of this stage is to measure the probability or possibility of occurrence of each of the risk events identified in the previous stage, as well as the impact in case of materializing through the associated risks. In the same way, the sources of information available to support the measurement process will be considered, based on the following:

Internal Information:

- Expert concept.
- Requirements of jurisdictional bodies.
- Reports of suspicious operations generated by the Company to the UIAF.
- Historical information on causes and/or risk events that allow semi-quantitative orientation of the risks to be evaluated.

External Information:

- Press publications.
- Firm sanctions carried out by the Superintendence of Corporations.
- Sanctions from other regulatory or supervisory bodies in matters of ML/TF/FPWMD.

For the measurement or assessment of the risk-managed, qualitative estimates are made based on the knowledge of experts, the experience of the employees involved, the Compliance Officer and advisors, and the practices and experience of the sector. The team of experts selected is expected to have knowledge and experience in the processes and risks to be analyzed.

3.2.1. SCALES OF MEASUREMENT

In order to determine the classification of the degree of risk managed for each of the events identified, the following probability table is used as a basis:

Score	Level	Estimated Occurrence	Data Historical Data
1	Unlikely	May occur exceptionally Less than 5% of the times the process is executed	Has not occurred in the last year
2	Occasional	May occur occasionally Between 5% - 10% of the times the process is executed	Has occurred less than 5 times in the last year
3	Possible	May occur at any time in the future Between 11% - 30% of the time the process is executed	Has occurred between 6 and 10 times in the last year.
4	Likely	Likely to occur Between 31% - 60% of the times the process is executed	Has occurred between 11 and 15 times in the last year.
5	Frequent	Occurs in most circumstances More than 60% of the times the process is executed	Has occurred more than 15 times in the last year

Probability Table.

The impact is determined based on the level of loss or damage that could result if the risk materializes and the associated risks (legal, reputational, operational, and contagion, among others), the impact table is defined in these terms:

Score	Level	Legal Risk	Reputational Risk	Operational Risk	Risk of Contagion
1	Insignificant	Requirement	Internal knowledge	May generate losses of less than 0.5% of EBITDA/Income	Does not affect the Company's operations
2	Minor	Reprimand, warning, administrative order.	Negative publicity	May generate losses between 0.6% and 1% of EBITDA/Income	Affects relations with third parties
3	Moderate	Fine or sanction	Loss of customers	May generate losses between 1.01% and 1.5% of EBITDA/Income	Affects one of the product lines
4	Major	Suspension	Nationally known legal proceedings	May generate losses between 1.6% and 2% of EBITDA/Income	Affects all product lines
5	Catastrophic	Closing	Internationally known	May generate losses greater than 2% of EBITDA/Income	Affects the entire Company's operations.

Impact Table

Subsequently, the Risk Severity level inherent to each risk event is determined, derived from the multiplication of the probability by the impact, obtaining a value from the following matrix (Heat Map) of:

Probability							
Frequent	5	10	15	20	25	Severity	Level
Likely	4	8	12	16	20	Extreme	16 - 25
Possible	3	6	9	12	15	High	10 - 15
Occasional	2	4	6	8	10	Moderate	5 - 9
Unlikely	1	2	3	4	5	Low	1 – 4
	Insignificant	Minor	Moderate	Major	Catastrophic		
					Impact		

3.2.2. RECORDING OF THE MEASUREMENT STAGE

It will be carried out in the Risk Matrix according to the following characteristics:

- Associated Risk – Risk Consequences: It will be understood as the dimension or impact of a risk against its associated risks (Legal, Reputational, Operational, Contagion, among others).
- Inherent Probability: It is established as the number of times a risk event can occur in a given period of time.
- Inherent Impact: The magnitude of the risk impact refers to the effects or consequences of the materialization of the risks identified in the Matrix.
- Inherent risk classification: Level of risk inherent to the normal development of the business.

ASSOCIATED RISK	INHERENT IMPACT	INHERENT PROB.	INHERENT RISK CLASSIFICATION

Once the inherent risks of the different identified risk events have been obtained, the methodology allows CCLA to know the level of exposure to the risks (Inherent Risk Profile), without taking into account the mitigation measures.

3.3. CONTROL STAGE

Controls are the mechanisms or activities that are implemented in the processes to mitigate risks and reasonably ensure that the Company's guidelines are carried out and risks are managed so that the objectives are met. For the definition of controls, the Risk Matrix is used as a basis, detecting those risks that require a control for their mitigation, either in the form of a policy or activity within the procedures.

During this stage, the methodology identifies the existing controls within the Company's processes, they are evaluated taking into account various attributes, and rated. At the end, the effectiveness of these is verified by evaluating the reduction of

impact and probability of risks, obtaining the measurement of the residual risk.

This methodology must be carried out through meetings with the participation of the different actors directly related to each of the processes where the risk is identified and the processes where the controls act. The controls are established by those responsible for the process with the support of the Compliance Officer or his team, incorporated in the existing CCLA procedures, and documented in the Risk Matrix.

In other words, the control must result in a reduction of the possibility of occurrence or impact of the managed risk, in case it materializes. The purpose of this stage is to take the necessary measures to control the risks, at this point CCLA must establish the residual risk profile.

3.3.1. DESIGN AND EFFECTIVENESS OF CONTROLS

At this stage, the control is determined as the measure taken to detect or reduce the probability of occurrence and/or the magnitude of impact if the risk materializes. Controls are incorporated into processes to ensure that workflow requirements and general service objectives are met. To carry out this stage, an inventory of controls will be made, including their respective description and valuation, in order to obtain the Residual Risk valuation, which allows for identifying the modification that took place for the risks.

In general, existing controls will be required to observe certain characteristics, which are considered necessary to contribute to the detection and reduction of risks:

- Sufficient: Elaborate on the appropriate amount.
- Timely: Existing when required.
- Understandable: Simple and clear.
- Effective: that they are both effective (allows risk to be detected and reduces the probability of its occurrence or impact) and efficient (correct use of resources for its application).
- Immersed in the processes: Assumes that the performance of activities includes control.
- Economic: It will be sought that its cost is lower than the benefit.

The evaluation of the design of each type of control will focus on the following aspects, which are considered essential, to which a value has been assigned to determine whether it is well designed or whether it should be redesigned. It is worth mentioning that controls can be of two types, Preventive Control, and Corrective Control, depending on whether they help to minimize the probability or mitigate the impact (Annex 1 contains the format of the forms that will be used to carry out the evaluation of the controls).

Evaluation of the design of the preventive risk

Criteria	Response	Score
Does the control have an assigned person responsible for its execution?	YES	1
	NO	0
Is the control documented/does it have physical evidence of its existence?	YES	1
	NO	0
Is evidence of control execution retained?	Always	1
	Sometimes	0.5
	Never	0
What type is the control execution?	Manual	0.5
	Automatic	1
	Hybrid	0.5
	None	0
Is there an established periodicity?	YES	1
	NO	0

Evaluation of the corrective/detective risk design

Criteria	Response	Score
Does the control have an assigned person?	YES	1
	NO	0
	YES	1

Is the control documented/does it have physical evidence of its existence?	NO	0
Is evidence of control execution retained?	Always	1
	Sometimes	0.5
	Never	0
What type is the control execution?	Manual	0.5
	Automatic	1
	Hybrid	0.5
	None	0
Are the resources for the execution of the control clearly defined?	YES	1
	NO	0

The table below indicates the valuation assigned to the weighted result of the score, which considers the same weight for each factor (15%).

The evaluation assigned to the design of the controls

Control Characteristics	Maximum Score	Minimum Score	Evaluation
The control complies with all the requirements	75.0%	60.1%	High
The control complies with some of the requirements	60.0%	40.1%	Medium
The control complies with a few of the requirements	40.0%	20.1%	Low
There is no defined control	20.0%	0.0%	Null

It should be noted that a score of 100% is not given to the controls since it is not considered that a control is completely effective and reduces the corresponding risk to zero. At the end of this stage, CCLA's residual risk map will be drawn up, which handles the same ranges as the inherent risk.

3.3.2. RESIDUAL RISK MEASUREMENT

Control qualifications as a whole allow for the evaluation of their effectiveness for risks. In this step it is possible to count on the collaboration of the process owners, determining if the control works in reducing the probability and/or impact.

With the previous result, it is possible to have a new qualification in the levels of probability and impact. In turn, these new qualifications must be placed in the qualification matrix, where the horizontal axis establishes the impact and the vertical axis the probability. According to the risk measurement methodology, the Company's residual risk level is defined.

The level of Severity to the residual risk, that is, the result of the exposure taking into account the effect of the controls over the identified inherent risks accepted by the Company is "MODERATE".

3.3.3. RECORDING OF THE CONTROL STAGE

The recording of the measurement of risks will be made in the Risk Matrix according to the following characteristics:

- Control: Measures taken for the mitigation of inherent risks.
- Control rating: Result of the control evaluation.
- Residual impact: The magnitude of the risk after the controls have been implemented for its mitigation.
- Residual probability: The number of times the risk event may occur after implementing controls.
- Residual risk classification: The level of risk inherent in the normal course of business, after controls have been implemented.

CONTROL	QUALIFICATION OF THE CONTROL	RESIDUAL IMPACT	RESIDUAL PROB.	CLASSIFICATION OF RESIDUAL RISK

3.4. MONITORING STAGE

After qualifying the controls, according to the results, the mitigation percentage is assigned for each risk, to determine by how much the inherent risk is reduced and what are the new values taken by the variables' frequency and impact, in order to establish whether the results required by management for the reduction of the risk profile were obtained. Monitoring will be carried out periodically, at least once a semester.

3.4.1. TYPES OF MONITORING

The monitoring that will be carried out will have different periodicities, such as:

- Specific monitoring: It is applied to processes and controls that require actions aimed at taking immediate corrective actions, either due to deficiencies or failures detected in the follow-up of performance indicators or as a result of audits. It is the verification of compliance and effectiveness of Risk Management Systems, the function of the conditions or characteristics of the model, standards, or defined policies, which are more selective and less frequent.

- Continuous monitoring: These are routine or check measures, subject to the particular responsibilities of each position established by CCLA through policies, standards, and procedures that are supported by the specific manuals of the product, channel, or service, among others, the above to apply controls, authorizations, restrictions or limitations immediately.

- Periodic monitoring: Refers to the review of the line of business and its controls, and corresponds to the management by managers or hierarchical level above the one executing the process and control. They are selective follow-ups in scope, but routine and/or regular that must be applied with a periodicity according to the weighted risk criteria, such as reporting to the various oversight and control bodies.

In this instance, the Company must compare the evolution of the inherent risk profile with the residual risk profile, as well as develop reports that allow establishing the evolution of the risk, such as the efficiency of the implemented controls.

Based on the results obtained in the previous phase, CCLA will carry out an effective follow-up process that facilitates the rapid detection and correction of the model's deficiencies, at least every six months; ensuring that the controls are comprehensive of all risks and that they are functioning in a timely, effective and efficient manner. For this purpose, the risk map is used, with the analysis of the effect of the controls on the inherent risk, in accordance with the following policies:

Level of Residual Severity	Policy	Treatment
Extreme	Under no circumstances will a risk of this level be accepted, therefore, the activity where a risk event of this level is located will be suspended while the corresponding treatment is given. These risks require high-priority attention from the Management where the event is located in order to immediately reduce its severity.	Immediate action is required, treatment plans are required, implemented, and reported to the corresponding body and to the Registered Agent.
High (Risk Tolerance)	Requires priority actions to be executed in the short term by the managers or directors of the departments responsible for the processes where the event occurs, due to the high effect it would have on the Entity.	Requires attention within three (3) months after its identification through treatment plans implemented and reported to the corresponding managers.

Moderate (Risk Tolerance)	Activities for the management of this risk must be implemented in the medium term by the assistants or coordinators of the department where the event is generated.	Acceptable risk managed with normal control procedures, requiring treatment within six (6) months after its identification, with a report to the corresponding managers.
Low (Risk Appetite)	The risk has a low severity; therefore it does not justify the investment of resources and does not require additional actions to those already established. Current actions must be retained to maintain the level of risk. These are monitored and reviewed every six months to ensure that the risk level has not increased.	Managed with routine procedures. Negligible risk, no action required.

3.4.2. ACTIVITIES OF THE MONITORING STAGE

The Monitoring stage includes the following activities:

- Analyzing reported indicator data.
- Establishing descriptive and/or prospective indicators that show potential sources of risk.
- Following up and comparing the inherent and residual risks of each risk factor and associated risks.
- Ensure that the residual risks are within the acceptance levels established by the Entity.
- Development of the follow-up process for the detection and correction of model deficiencies. Based on the results, improvement plans will be developed.
- Ensure that the controls of all risks are comprehensive and for this purpose an assessment verification will be carried out according to the nature of

the risk, considering manual, automatic, and technology-dependent controls.
- Evaluate the relevance of the indicators.
- Compliance evaluation of the objectives and policies of the System.
- Evaluate the result of the indicator diagnosis and follow up on the previous result.
- Communicate results to the responsible manager.
- Prepare a report of the results generated.

3.5. IMPROVEMENT ACTIONS

It is a formal and documented process, coordinated by the Compliance Officer and his team to implement actions to reduce the Severity level of residual risks. The improvement action plan identifies responsibilities, schedules, proposed actions, and the established review process. To perform an effective follow-up on the strengthening of controls to reduce the frequency and impact of risks, the Compliance Officer and his team record the improvement action plans in the following matrix:

No.	Risk Name	Risk Description	Residual Risk
Event Code	Activity/Description Short Event Name	Activity/ Characterization and Description of the Inherent Risk	

Improvement actions				
Policy	Proposed Actions	Responsible	Date	Monitoring

ANNEX 1.

PREVENTIVE CONTROL EVALUATION

Control _____
Process _____
Procedure _____
Risk _____
Responsible _____

	Criteria	Response	
15%	Does the control have an assigned person?	YES	
		NO	
15%	Is the control documented/does it have physical evidence of its existence?	YES	
		NO	
15%	Is evidence of control execution retained?	Always	
		Sometimes	
		Never	
15%	What type is the control execution?	Manual	
		Automatic	
		Hybrid	
		None	
15%	Is there an established periodicity?	YES	
		NO	

CORRECTIVE CONTROL EVALUATION

Control _____
Process _____
Procedure _____
Risk _____
Responsible _____

	Criteria	Response
15%		YES

	Does the control have an assigned person?	NO	
15%	Is the control documented/does it have physical evidence of its existence?	YES	
		NO	
15%	Is evidence of control execution retained?	Always	
		Sometimes	
		Never	
15%	What type is the control execution?	Manual	
		Automatic	
		Hybrid	
		None	
15%	Are the resources for the execution of the control clearly defined?	YES	
		NO	