AIAC Investment Advisors SA, Trust Company

VIGILADO SUPERINTENDENCIA FINANCIERA DE COLOMBIA

INTEGRATED RISK MANAGEMENT SYSTEM (SIAR)

Ashmore Investment Advisors S.A.
Trust Company

2025

INDEX OF MODIFICATIONS			
Version	**Modified or Added Clause**	**Date of Modification by Board of Directors (dd/mm/yyyy)**	**Description**
0.0	Document Creation	18/05/2023	Document creation.
1.0	Update	26/10/2023	-Update the Market Risk Management section of Part II of the Trust's SIAR Manual by referencing the sections of Chapter XXXI "SIAR" of the Basic Accounting and Financial Circular - General numbering of the document
2.0	Update	15/05/2025	Annual system review. No material changes were found.
3.0	Update	04/09/2025	-Incorporation of a new chapter on credit risk and update of Part IV definitions
4.0	Update	15/11/2025	-Incorporation of a new chapter on conduct risk.

Ashmore

CONTENT

Section ..... Page

PART I. GENERALITIES OF THE INTEGRATED RISK MANAGEMENT SYSTEM (SIAR) 7

1. INTRODUCTION 7

1.1. Objectives of SIAR 7

2. COMPONENTS OF SIAR 8

2.1. Risk Appetite Framework (RAF) 8

2.2. SIAR Stages 9

2.3. SIAR Policies 9

2.3.1. Risk Management 10

2.3.2. Risk Management Procedures 11

2.3.3. Information 12

3. RISK GOVERNANCE STRUCTURE 12

3.1. Board of Directors 12

3.2. Legal Representative 14

3.2.1. Risk Management 14

3.2.2. Reports and information 14

3.3. Risk Management Area or Position 15

3.3.1. Functions of the Risk Management Area or Position 15

3.3.2. Reports and information 16

3.4. Risk Committee 17

3.4.1. Composition 17

3.4.2. Functions 17

3.5. Internal Audit 18

3.6. Statutory Auditor 18

4. TECHNOLOGICAL INFRASTRUCTURE AND INFORMATION SYSTEMS 19

4.1. Minimum requirements of the technological infrastructure of Entity 19

4.2. Internal Information 19

4.3. External Information 20

4.4. Documentation 20

PART II. RISK MANAGEMENT 21

1. MARKET RISK MANAGEMENT 21

1.1. Definition of market risk 21
1.2. Components 21
1.2.1. Stages 21
1.2.2. Limits 24
1.3. Disclosure of information and reports 25
1.3.1. Internal Disclosure 26
1.3.2. External Disclosure 26
1.4. Documentation 27
2. OPERATIONAL RISK MANAGEMENT 28
2.1. Definition of operational risk 28
2.2. Components 28
2.2.1. Stages 28
2.2.2. Training 39
2.3. Special rules regarding attachment orders 39
2.3.1. Reception 40
2.3.2. Processing 40
2.3.3. Timely Attention and Response 41
2.3.4. Compliance 42
2.3.5. Conservation and Archiving of Information 43
3. LIQUIDITY RISK MANAGEMENT 43
3.1. Definition of liquidity risk 43
3.2. Components 44
3.2.1. Stages 44
3.3. Limits 50
3.4. Liquidity Contingency Plan 51
4. COUNTRY RISK MANAGEMENT 52
4.1. Definition of country risk 52
4.2. Components 53
4.2.1. Stages 53
4.2.2. Reports 57
5. CONDUCT RISK MANAGEMENT 57-60
5.1. Definition of Conduct Risk 57
5.2. Scope and Application 58

5.3. Guiding Principles 58
5.4. Key Factors of Conduct Risk 59
5.5. Relevant Sources of Conduct Risk for the Company 59
5.6. Controls and Mitigation Measures 59
5.7. Monitoring and Reporting 60
5.8. Responsibilities 60
6. CREDIT RISK MANAGEMENT 60
6.1. Definition of credit risk 60
6.2. Scope and Application of SARC 60
6.3. Exceptions 61
6.4. Stages of the Credit Risk Management System 62
6.4.1. Identification 62
6.4.2. Measurement 62
6.4.3. Control 64
6.4.4. Monitoring 64
7. CREDIT EXPOSURE ACCEPTANCE AND MONITORING CYCLE 65
7.1. Admission of counterparties and issuers 65
7.2. Prior information and transparency 65
7.3. Assessment of payment capacity 65
7.4. Evaluation and assessment of guarantees 65
7.5. Monitoring and control 65
7.6. Management of deterioration situations 65
8. EXPOSURE LIMITS AND MONITORING 65
9. ROLES AND RESPONSIBILITIES IN SARC 66
9.1. Board of Directors (BD) 67
9.2. Legal Representative (RL) 67
9.3. Financial Risk Unit 67
9.4. Risk Committee 68
9.5. Control Bodies 68
9.6. Statutory Audit 69
9.7. Internal Audit 69
10. TECHNOLOGICAL INFRASTRUCTURE AND INFORMATION SYSTEMS 69
Main technological tools 69

Controls and responsibilities 69
11. CONTINUITY AND CONTINGENCY PLANS 70
12. SUPERVISION BY THE SFC 70
13. AGGREGATION OF RISK DATA AND REPORTING 71
13.1. Definition of risk data aggregation 71
13.2. Principles 71
PART III. STANDARD RISK MEASUREMENT AND REPORTING 71
1. INTRODUCTION 71
2. MARKET RISK MODEL 71
2.1. Measurement methodology - Standard measurement model 71
2.2. Accounting Disclosure 72
2.2.1. Qualitative Information 72
2.2.2. Quantitative Information 72
2.3. Reports to the SFC 72
3. MODEL FOR MEASURING AND RECORDING OPERATIONAL RISK EVENTS 73
3.1. Measurement Model 73
3.2. High-quality operational risk event log 73
3.2.1. General criteria for the recording of operational risk events 73
3.3. Accounting disclosure 76
3.4. Reports to the SFC 76
4. LIQUIDITY RISK MODEL 76
4.1. Measurement methodology 76
4.2. Accounting disclosure 76
4.3. Reports to the SFC 76
5. COUNTRY RISK MODEL 77
5.1. Disclosure of country risk 77
PART IV. DEFINITIONS 77

PART I. GENERALITIES OF THE INTEGRATED RISK MANAGEMENT SYSTEM (SIAR)

1. INTRODUCTION

External Circular No. 018 of 2021 ("Circular 018") of the Financial Superintendency of Colombia ("SFC") established the Comprehensive Risk Management System (SIAR), which aims to design, implement, and maintain a set of policies, strategies, practices, procedures, methodologies, controls, and/or limits for risk management. To implement a SIAR manual that complies with the provisions of Circular 018, ASHMORE INVESTMENT ADVISORS SA SOCIEDAD FIDUCIARIA ("AIAC," or the "Company") has undertaken an integration exercise of the documentation that forms part of its current Risk Management Systems.

The Integrated Risk Assessment System (SIAR) developed for AIAC was designed considering the company's risk profile and appetite, business plan, nature, size, complexity, and diversity of activities, and was presented to the Board of Directors by AIAC's Management. Furthermore, other factors, such as the economic environment in which the company operates, were considered in the preparation of this document and, in general, all AIAC's risk management policies and procedures.

The manual should be reviewed annually and updated as needed to incorporate material changes.

1.1. SIAR Objectives

The main objectives of the SIAR described within this document are:

A. Establish and promote a culture of risk.

B. Design, implement and monitor the risk appetite framework and the strategy for its execution.

C. Align risk management with the business plan, capital and liquidity levels, and risk appetite.

D. Identify, measure, control, monitor and report in a timely and comprehensive manner the risks inherent in the development of the business, including those derived from the management of third-party assets.

E. Contribute to the assessment of capital adequacy and liquidity.

F. Maintain consistency between its risk management policies and those of its subsidiaries, where applicable.

2. SIAR COMPONENTS

2.1. Risk Appetite Framework (RAF)

As an essential part of the SIAR, AIAC has developed the Risk Appetite Framework (" **RAF** ") (See Annex), that is, the levels and types of risks that it is willing to assume in order to comply with the business plan in accordance with the provisions of External Circular 018 of 2021 of the Financial Superintendency of Colombia and in Chapter XXXI of the Basic Accounting and Financial Circular of the Financial Superintendency of Colombia, or any regulation that modifies, repeals or adds to them, which indicates that the RAF is the set of policies, methodologies, procedures, controls and thresholds and/or limits from which ASHMORE: (i) identifies the risks associated with the business plan; (ii) evaluates whether said risks are assumed, mitigated, avoided or transferred, and (iii) monitors and controls that said risks are within the thresholds and/or limits defined by Senior Management (" **SM** ") and approved by the Board of Directors (" **BOD** ").

In accordance with the above, the following was taken into consideration for the development of the AIAC MAR:

A. AIAC's business plan and expectations of changes in its products and services offered that may modify its risk profile, capital levels and liquidity.

B. The regulatory obligations and requirements applicable to ASHMORE.

C. The current market and economic conditions of the Entity and the jurisdictions where it operates.

D. The losses or levels of risk that AIAC is willing to assume, capital analysis, profitability, volatility and/or liquidity, among other qualitative and quantitative elements.

E. Prospective analysis that allows AIC to anticipate and prepare for the potential materialization of risks in both normal and adverse scenarios.

F. The controls, thresholds and/or limits applicable in case of losses and/or the levels of risk that AIAC is willing to assume were defined, which includes an analysis of the capacity and tolerance to the risks assumed.

G. Both the General Administration and the Board of Directors will consider the SIAR and its development to carry out the evaluation and monitoring of the risks identified and found in the Entity's Operational Risk Matrix ("ORM").

Once approved by the AIAC Board of Directors through Senior Management, the SIAR must be disseminated and its understanding ensured to all employees, Internal Audit, the Risk Committee, the Audit Committee, the Statutory Auditor, and any other internal or external body deemed

appropriate for the proper and harmonious implementation of the SIAR. Furthermore, Senior Management must ensure that any modifications or updates to this document are disseminated as described in this section.

2.2. SIAR Stages

AIAC's Integrated Risk Assessment System (SIAR) includes a separate section detailing the analysis, policies, and procedures for managing each of the risks to which it is exposed. AIAC thus included the analysis of: (i) Market Risk; (ii) Operational Risk; (iii) Liquidity Risk; and (iv) Country Risk. This analysis was conducted considering the following general principles regarding risk:

A. Identification: This stage involves AIAC determining the risks (current and potential) inherent in the activities it carries out or plans to carry out. The Entity must conduct a new risk identification analysis beforehand in the case of new products or services or substantial modifications to current products and services.

B. Measurement: This consists of the stage developed by AIAC to quantify and/or evaluate exposure to the risks inherent in the activities that the Entity carries out or plans to carry out, and their impact should they materialize. This measurement must be qualitative and/or quantitative.

C. Control: This is the stage where AIAC has developed mechanisms to mitigate and/or minimize the possibility and impact of the materialization of risks inherent in its activities. These controls have been developed in such a way that the Entity can determine its level of compliance with its policies, strategies, procedures, methodologies, controls, thresholds and/or limits, and regulatory framework, as well as have access to updated, reliable, timely, and complete information.

D. Monitoring: This involves the continuous and effective tracking of risk sources, the risk profile, deviations from limits and/or thresholds, the effectiveness of implemented controls, and the potential impact of risk materialization. Additionally, it should facilitate the rapid detection and correction of deficiencies in ASHMORE's Risk Assessment System (RIA). Monitoring should be intensive regarding identified deficiencies in risk management and corrective and improvement actions.

2.3. SIAR Policies

Without prejudice to the specific sections on each of the risks, the generalities of the different SIAR policies and procedures adopted by AIAC, on which the management of its risks is based, are developed below.

2.3.1. Risk Management

A. AIAC shall implement the different stages of the SIAR and its elements within this document in accordance with the provisions of Section 2.2 above.

B. The Entity's Risk Management area, in conjunction with the General Management, must review the suitability and operation of the Integrated Risk Management System (SIAR) at least once a year and update it as necessary. It is important to note that if deficiencies and/or opportunities for improvement are identified, AIAC must ensure that these are included in the annual updates. Therefore, it will only be necessary to modify or update the SIAR within a shorter timeframe if the General Management considers that such a modification or update is material and could have an adverse effect on the Entity's comprehensive risk management.

C. Without prejudice to the obligations established for each of ASHMORE's social bodies, the Entity must ensure that there is approval of the activities it carries out or those it intends to carry out or modify.

D. As mentioned previously, ensure that the inherent risks of new markets, processes, and/or activities are identified.

E. AIAC shall define, monitor and report the MAR thresholds and limits and maximum levels of exposure, concentration and tolerated loss by type of risk, with a breakdown of positions by economic sector, activity, term, type of operation, reinsurer, counterparty, related parties, geographical area and currency, when applicable.

F. AIAC must have criteria for requiring, accepting, and appraising guarantees and counter-guarantees, when applicable.

G. AIAC shall take and implement the necessary actions, including disciplinary measures, in response to: (i) unexpected changes in risk exposure, (ii) activation of the early warning system, and (iii) breaches of internal and/or regulatory limits. It shall also implement guidelines regarding when and to whom the events are escalated and reported.

H. The Entity will implement the necessary measures in response to the materialization of risks and will periodically review the effectiveness of these measures.

I. AIAC shall design and implement contingency plans and business continuity management and plan, as well as conduct periodic reviews of the effectiveness of said plans, in accordance with the periodicity established by ASHMORE.

J. AIAC will manage the operational risk event log.

K. AIAC must contract insurance and outsource the development of its processes to natural and/or

legal persons, if it does not imply the delegation of professionalism.

AIAC must ensure the disclosure of the SIAR and MAR to the Board of Directors, the General Manager, those responsible for risk management, the risk committee, the statutory auditor, internal audit, and its business units. Likewise, the Entity must disseminate the policies and elements of the SIAR, including the guidelines established in AIAC's Code of Conduct and Corporate Governance Code, which will promote a risk culture and enable corrective and improvement measures to be taken in case of non-compliance.

2.3.2. Risk Management Procedures

For proper risk management, AIAC will ensure that the following guidelines and directives are met:

A. Allocate the necessary personnel and physical, financial, and technological resources for the development, implementation, and proper maintenance of the SIAR (Integrated System for Risk Assessment), as well as the minimum requirements these resources must meet. This will be done in accordance with the Entity's specific circumstances, activities, and human resources, ensuring sufficient resources without incurring unnecessary costs.

B. The Entity must provide at least annual training for its employees to strengthen their skills in risk management and to ensure the effective execution of the functions assigned to each of them.

C. The Code of Conduct and the Code of Good Corporate Governance are the policies and guidelines that all AIAC employees must follow, which complement and provide guidelines for the effective and timely operation of SIAR.

D. AIAC must ensure that the Entity's objectives and business plan correspond to the levels of capital and liquidity, and that these in turn correspond to the MAR defined by the Entity.

E. Any conflicts of interest that may arise must be identified, managed, disclosed, communicated and resolved in accordance with ASHMORE's Code of Conduct and Corporate Governance Code and current legislation on the matter.

F. Intragroup transactions arising with AIAC Affiliates must be managed, communicated and approved in accordance with the Code of Conduct and the Code of Good Corporate Governance.

G. Adapt AIAC's current internal control system to the requirements of SIAR.

H. The commercial incentives that are established must be aligned with a prudent assumption of risk, with the MAR, the long-term objectives, capital levels and liquidity of the Entity.

2.3.3. Information

Risk management systems require constant communication and that the various officials keep the General Manager, the Board of Directors, the Risk Committee, the Audit Committee, and any other relevant bodies, as well as external entities as determined by the Entity, informed. In this way, the following will be considered as a minimum:

A. Communicate to the Board of Directors, Risk Committee and the General Management about risk management, as well as the findings and recommendations of those who perform the risk management function, Internal Audit and the Statutory Auditor.

B. To attend to the information requests from the SFC and/or other competent authorities, as well as to have mechanisms to validate the quality of the information provided.

3. RISK GOVERNANCE STRUCTURE

The Entity must have an appropriate organizational structure for risk management and compliance with the SIAR (Integrated Risk Assessment System), which must be aligned with the business and risks to which it is exposed. This structure must include:

A. The procedures that allow the Entity to make informed decisions, manage risks, design and monitor the SIAR, and report and accountability.

B. Clearly defined roles and responsibilities for AIAC areas and staff involved in risk management, as well as procedures for evaluating their performance.

AIAC's business units, if any, must be part of the comprehensive risk management system, given that they assume and/or generate exposure to one or more risks and are therefore responsible for their ongoing management. Consequently, risk management policies, practices, strategies, procedures, methodologies, models, and thresholds and/or limits must be integrated with the products and services offered by AIAC.

3.1. Board of Directors

The Board of Directors must fulfil at least the following functions and responsibilities:

A. Approve AIAC's Business Plan, verify its compliance, and consider and approve any related modifications.

B. Approve and verify compliance with the MAR, SIAR policies, general exposure and concentration limits, the risk governance structure, and strategies for managing: (i) risks, (ii) capital, (iii) liquidity, and (iv) conflicts of interest and their disclosure; as well as any updates thereto. To do so, verify that these are consistent with the risk profile and appetite, the business

plan, the nature, size, complexity, and diversity of the entity's activities, and the economic environments and markets in which AIAC operates.

C. Approve: (i) the guidelines for internal reports submitted to it in relation to risk management and (ii) the liquidity contingency plan; as well as its updates.

D. Approve the measures to be implemented and monitor their application and effectiveness when the following occur: (i) increases in exposure to risks that result in exceedances of the regulatory and/or internal thresholds and/or limits defined by the Entity or non-compliance with the MAR, (ii) weaknesses in the SIAR to manage risks in accordance with the economies and market in which the Entity operates, its level of capital and liquidity, the regulatory framework, the business plan and AIAC's risk profile and appetite, and (iii) corrective and improvement actions, once the previous instances in the governance structure have been overcome.

E. To know the results of the stress tests and approve the measures or plans to be implemented to mitigate the risks based on their results.

F. Monitor, at least once a year, the effectiveness and suitability of the SIAR to carry out adequate risk management and its consistency with the business plan and with the economies and markets in which the Entity operates, as well as approve improvement actions.

G. Prior approval is required for the reclassification of a position in the treasury or bank ledger because of an identified hedging strategy. The reclassification will only take effect 30 business days after its adoption. This does not imply or permit the reclassification of investments for valuation and accounting purposes, the rules for which are set forth in the Investment Valuation Chapter of the Basic Accounting and Financial Circular (CBCF) or any regulation that modifies, adds to, or repeals it. In any case, the hedging strategies to be implemented must comply with the criteria defined in Chapter XVIII of the CBCF or any regulation that modifies, adds to, or repeals it.

H. Appoint the members who are part of the risk committee, approve its regulations and define its functions.

I. Approve, at least once a year, the training policy for personnel who are part of the Entity's risk governance structure, as well as the guidelines on ethics or conduct and internal control related to the SIAR.

J. The decisions made by the Board of Directors in the exercise of the powers must be recorded in writing in the minutes of the respective meeting and be duly justified.

3.2. Legal representative

The legal representative must, under the direction and supervision of the Board of Directors, execute and monitor the implementation and compliance of the business plan and the SIAR, which is why they must at least fulfil the following functions and responsibilities:

3.2.1. Risk management

A. Submit the business plan, the MAR, the SIAR policies, the general exposure and concentration limits, the risk governance structure, and the strategies for managing (i) risks, (ii) capital, (iii) liquidity, and (iv) conflicts of interest and their disclosure, as well as any updates, to the Board of Directors for approval. Likewise, ensure compliance with these requirements.

B. Submit to the Board of Directors for approval: (i) the guidelines for internal reports submitted to it in relation to risk management and (ii) the liquidity contingency plan when required; as well as its updates.

C. Approve the SIAR manual and the contingency and business continuity plans. The latter must address the risks associated with interconnectivity with other infrastructures and/or supervised entities or suppliers (third parties).

D. Verify that contingency and business continuity plans are included in the budget for their timely implementation.

E. Monitor that the SIAR is adequate for managing risks and is in accordance with the profile and risk appetite, business plan, nature, size and complexity of the Entity, the regulatory framework and the conditions of the economies and markets in which it operates.

F. Periodically review the composition, characteristics and level of diversification of assets, liabilities, capital, liquidity and funding strategy.

G. Ensure that the operational risk event log meets the criteria of integrity, reliability, availability, compliance, effectiveness, efficiency and confidentiality of the information contained therein, as well as ensuring that there is a procedure for feeding said log.

H. To strive for the quality and consistency of information.

3.2.2. Reports and information

A. Report quarterly to the Board of Directors on the Entity's performance, its financial situation and the problems identified in risk management along with the respective recommendations.

B. Inform the Board of Directors promptly about: (i) changes or deviations from the business plan and risk appetite, (ii) any risk situation or event that may compromise the viability of the business or public confidence and ensure that corrective measures and/or improvement actions are taken.

C. Inform the SFC promptly about any situation or risk event that compromises the viability of the business or public confidence, as well as the causes that originated it and the measures that will be put in place to correct or address said situation.

D. Notify the SFC in writing within 10 business days following the authorization of the operation contemplated in Section 0 above, in the event of such reclassification of a position.

3.3. Risk Management Area or Position

The Entity must have a risk management area or position to carry out such management, ensuring its organizational independence from business units, technology areas, and other departments that could generate conflicts of interest. The person(s) performing this function must: (i) have direct access to the Board of Directors, the Risk Committee, the General Management, business units, and other departments of the Entity, as well as to their records and information; and (ii) have the hierarchical level, decision-making power, and sufficient authority to fulfil their functions and responsibilities and to make recommendations and monitor the measures taken by management in response to identified problems and opportunities for improvement.

Notwithstanding the foregoing, AIAC will also consider the nature, size, and complexity of the activities it carries out to designate the appropriate person(s). Those responsible for risk management within the Entity must fulfil at least the following functions and responsibilities:

3.3.1. Functions of the Risk Management Area or Position

A. Prepare, together with the legal representative of the MAR, the SIAR manual and its updates.

B. Develop the policies, procedures, strategies, methodologies, models, thresholds and/or limits, controls, contingency plans, business continuity plan, and early warning and monitoring indicator framework for the MAR. Submit any relevant updates to the legal representative.

C. Evaluate, in coordination with other areas involved in risk management, contingency and business continuity plans, risk exposure and management, and any deviations from established limits and risk appetite, as well as their alignment with capital and liquidity levels. This should include the risks inherent in new activities and/or markets, and their impact on the Entity's risk profile and management.

D. Monitor the influence of related party funding positions and characteristics on the Entity's liquidity risk.

E. To make pronouncements on operations that do not comply with the policies, controls and/or risk limits established by the Entity or within the regulatory framework and report them as soon as possible to the legal representative and those responsible for the business units.

F. Conduct stress tests to establish the Entity's potential risk exposures under a variety of scenarios and design the measures or plans to be implemented to mitigate the risks based on the results.

G. Compare the results of the stress tests against the risk appetite levels and identify the corresponding risk mitigation actions and report the results to the Board of Directors, the legal representative and the risk committee.

H. Manage the operational risk event log and coordinate the collection of information for said log and, from this, generate information that contributes to risk management.

3.3.2. Reports and information

A. Report quarterly to the Board of Directors on the nature and level of the Entity's risks and their consistency with its risk appetite and capital and liquidity levels, including potential outcomes under extreme conditions based on reasonable assumptions. In any case, the Board must be promptly informed of any significant increases in risk exposure, as well as their impact on current and future capital and liquidity levels.

B. Report monthly to the legal representative and to the risk committee:

   a. The entity's risk exposure must be detailed, at a minimum, by the specific exposure for each significant activity and by risk, its deviations from established limits, and its correlation with capital and liquidity levels, where applicable. Reports on liquidity risk exposure must include the quantification of cash flow mismatches or imbalances compared to the amount of liquid assets available to the entity, with particular emphasis on transactions with entities within the financial conglomerate and with related parties, as well as a sensitivity analysis and stress testing under extreme conditions based on reasonable assumptions.

   b. In the case of counterparty risk, the overall concentration level, segmented by type of guarantee backing the client's current fulfilment operations, must be provided. This information must be broken down at least by term, type of transaction, and type of counterparty.

C. Report semi-annually to the Board of Directors, the risk committee, and the legal representative on the evolution of operational risk, the controls implemented, and the monitoring carried out on it, as well as the preventive and corrective actions implemented or to be implemented and the

responsible area.

D. Report to the legal representative and those responsible for the business units:

E. At least once a day, and depending on the type of business or activity, the behaviour of market risk and liquidity.

F. Weekly, market risk levels, the conditions of the negotiations carried out and breaches of limits, unconventional or off-market transactions, and transactions with related parties.

G. Ensure that the Board of Directors, the General Manager, and the risk committee are promptly and properly informed about:

H. Non-compliance with the MAR, internal and/or regulatory thresholds and/or limits and propose the corresponding corrective measures.

I. Changes in the economic, political and market environment, both local and external, that may affect the Entity's current and future risk profile and/or compromise compliance with the SIAR limits and policies.

J. The risks inherent in new activities and/or markets and their impact on the Entity's risk profile and management and on capital and liquidity levels.

K. Report in a timely and understandable manner to the AG and to the heads of the business units, the problems identified in risk management along with the respective recommendations.

3.4. Risk Committee

3.4.1. Composition

The Risk Committee will consist of an odd number of members (3) and will meet regularly at least once every three months. The Committee will be chaired by an independent member of the Board of Directors. Members will also have knowledge and experience in risk management. The person directly responsible for the risk management function will support the Committee.

3.4.2. Functions

The AIAC Risk Committee must fulfil at least the following functions and responsibilities:

A. Monitor the Entity's risk profile and appetite, as well as assess its consistency with the business plan, capital and liquidity levels, and report to the Board on the main results and issue the corresponding recommendations, when necessary.

B. Advise the Board on transactions, events or activities, including entry into new markets, that may (i) affect the entity's risk exposure and profile, (ii) constitute deviations from the business plan, risk appetite and internal and regulatory limits or (iii) compromise the viability of the business.

C. Review SIAR policies at least once a year and propose the corresponding adjustments to the Board of Directors for their respective approval.

D. Advise the Board of Directors on the state of the risk culture in the Entity.

E. Evaluate the suitability of the business continuity plan and contingency plans.

F. Inform the Board of Directors of your analysis of the results of the monthly reports received from those who perform the risk management function.

3.5. Internal Audit

Without prejudice to the functions and responsibilities set forth in Chapter IV of Title I of Part I of the CBJ, the AIAC Internal Audit is responsible for:

A. Periodically evaluate the effectiveness and compliance of the SIAR (Integrated Risk Management System), or whenever situations arise that require its review, and inform the person(s) responsible for risk management, the legal representative, the audit committee, and the Board of Directors of the results of said evaluation, as well as the follow-up on recommendations, improvement actions, and compliance with the audit plan. This evaluation must expressly cover, at a minimum, the operations and liquidity flow to and from related parties.

B. Follow up on the recommendations or failures identified in risk management resulting from the SFC assessments and the internal audit itself, as well as the action plans and measures adopted by the Entity.

C. Inform the SFC of situations whose materiality may affect the development of the business and the corrective and improvement actions that have not been addressed by the Entity.

The evaluation carried out by the Internal Audit regarding the SIAR must respond to changes in the environment and in the risk profile of the Entity, as well as be based on the risks that it faces.

3.6. Statutory Auditor

Without prejudice to the functions assigned in other legal provisions, AIAC's Statutory Auditor must include in their audit plan the periodic evaluation of compliance with SIAR instructions and must prepare an Annual Report with the conclusions obtained in the evaluation and review process, which must be included in the opinion on the financial statements. These reports will be available to the SFC.

Likewise, Ashmore's Statutory Auditor must promptly inform: (i) AIAC's Shareholders' Meeting, (ii) the Board of Directors, (iii) the legal representative, and (iv) the SFC, of any material irregularities observed in compliance with the instructions established in the SIAR and any deficiencies found in internal controls. This report must be properly documented, including the results achieved, the actions suggested, and the Entity's response to the observations.

4. TECHNOLOGICAL INFRASTRUCTURE AND INFORMATION SYSTEMS

AIAC will have the systems, technological support and data architecture that allow a comprehensive view of the risks, the operation of the SIAR, the presentation of reports, decision-making, as well as compliance with regulatory requirements.

4.1. Minimum requirements for the technological infrastructure of the Entity

A. A system of internal and external reports, in accordance with the size, nature and complexity of the operations carried out by the entity.

B. Procedures for handling and storing information that ensure its confidentiality, security, quality, availability, integrity, consistency, and consolidation.

C. Up-to-date databases and sufficient and timely information to carry out risk management.

D. General guidelines for the aggregation of risk data and presentation of information of the Entity.

The area responsible for carrying out the validation and testing will send a report to the Entity's Risk Committee, or failing that, to the legal representative, which includes a description of the methodology used for the validation and testing, its results, and the identification of possible improvement actions.

4.2. Internal information

The Entity will prepare periodic reports that allow it to: (i) establish and understand its risk profile in normal and adverse scenarios and the correspondence with risk appetite, asset and liability structure, capital and liquidity levels, business plan and the conditions of the economies and markets in which it operates, (ii) anticipate problems, (iii) make informed decisions and (iv) provide an assessment of risk management.

The content and frequency of risk management reports, as outlined in this document, will reflect the needs of the recipients and the nature of the reported risk. Reporting frequency should increase in adverse scenarios. These reports will disclose the hypotheses or assumptions used to present the information and any limitations in the risk assessment.

Additionally, the area or person(s) responsible for Risk Management within the Entity will prepare an

annual management report on the functions performed in this area. This management report must be presented to the Board of Directors and the legal representative in a clear and understandable manner.

4.3. External information

In accordance with Article 97 of the Organic Statute of the Financial System (EOSF) and other applicable legal provisions, the Entity will provide the public with the necessary information to enable them to choose the best options and make informed decisions. The information disclosed to the public will be consistent with the size, complexity, nature, and risk profile of the Entity's activities. Likewise, the Entity will submit the information to the SFC in accordance with the terms established in this article and other related regulations.

4.4. Documentation

The entity will have at least the following documentation:

A. The minutes by which the Board approves the SIAR, and the other specific points designated to it in this Manual.

B. The logbook in which the updates and modifications of the SIAR and the MAR are recorded.

C. Risk models.

D. The business continuity plan and contingency plans.

E. The early warning system and other indicators implemented for monitoring each risk, as well as the actions, corrective and improvement measures implemented in response to non-compliance with limits or activation of alarms.

F. Reports prepared by the different risk management bodies and officials of the government in relation to risk management and other documents that support the monitoring of said management.

G. The Code of Conduct and the Code of Good Corporate Governance.

H. The organizational structure of risk governance.

I. The operational risk event log.

This SIAR Manual will be duly documented, backed up in verifiable media, and have a plan for the conservation, custody, and security of the information, so that it is only allowed to be consulted by authorized officials.

PART II. RISK MANAGEMENT

1. MARKET RISK MANAGEMENT

1.1. Definition of market risk

Market risk is understood as the possibility that entities may incur losses associated with the decrease in the value of their portfolios, the falls in the value of collective investment funds (formerly collective portfolios) or funds that they manage, due to changes in the price of financial instruments in which positions are held within or outside the balance sheet.

1.2. Components

1.2.1. Stages

1.2.1.1. ID

The Entity identifies the market risk to which it is exposed, based on the type of positions assumed, in accordance with the authorized operations, the business plan and risk appetite defined by the Entity.

The Entity is a Trust Company that will primarily engage in investment trust activities and, in this sense, will enter into fiduciary assignments (“Fiduciary Assignments”) or commercial trusts (“Commercial Trusts”), in order to discretionally manage clients' portfolios and act as the principal of their resources, which is why it is exposed to market risk and all its risk factors, which are:

A. Interest rate in legal tender.

B. Foreign currency interest rate.

C. Interest rate in transactions agreed at a variable rate, i.e., indexed to UVR, CPI or IBR, among other UVR.

D. Exchange rate.

E. Stock price.

F. FICs.

This stage will be carried out prior to participation in new markets and the negotiation of new products, determining their risk profile and quantifying the impact they have on the level of risk exposure of the

Entity, its equity and profits.

1.2.1.2. Measurement

The Entity must have an information system and methodologies appropriate to the complexity and level of risks involved in its activities, enabling it to measure and quantify expected losses arising from market risk exposure, in accordance with the following instructions. Considering the following:

a. It must measure its exposure to market risk arising from its treasury book positions and cash transactions, as well as from the various investment funds and other funds it manages. To this end, it must implement the standard market risk measurement model, report the measurement results, and comply with the limits and measures, in accordance with the instructions set forth in section 3 of Part III of Chapter XXXI of the CBFC.

b. In the case of trusts managed by trust companies that invest exclusively in the investment funds of the same management company, these investments are exempt from implementing the standard model. Funds are also exempt from using the standard model when the settlor expressly indicates in writing their intention to apply a different measurement model or exempts the entity from this obligation.

AIAC adopts the standard market risk model proposed by the Financial Superintendency of Colombia (Annex A of the risk appetite framework)

1.2.1.2.1. Stress tests

As part of its normal business operations, the entity conducts stress tests to assess its capacity to absorb losses in adverse market scenarios that could affect the value of its portfolios. These tests must consider extreme scenarios for each risk factor to quantify, over different time horizons and depending on the type of position held, the potential impact of market risks materializing on the entity's risk exposure, capital, and earnings. If structural market changes occur that are not adequately reflected in the historical data series used, the tests must account for these movements in the risk factors.

The designed and implemented models must be statistically robust and serve as input for risk management decision-making. Additionally, the test results should generate indicators that trigger the corresponding contingency plan.

Stress tests, their review, and updates must be performed at least quarterly. The Entity may increase the frequency of the tests under special scenarios such as changes in market conditions, crises, or at the request of the SFC, to whom it must disclose the assumptions, parameters, analysis, measurement, and results of these tests.

The results of the stress tests carried out by the Entity must be available to the SFC for consultation at any time.

1.2.1.3. Control

The Entity will design and adopt measures to control the market risk to which it is exposed in the development of its operations.

Market risk control must at least meet the following requirements:

A. Be proportional to the volume and complexity of the operations carried out by the entity, so that there is a correspondence between the model and the operations carried out.

B. To allow for the control of market risk exposure levels and the general limits established by the entity, as well as the specific limits determined for treasury activity at the trader, trading desk, and product levels. This is in accordance with the structure, characteristics, and operations authorized for each type of entity.

C. Allow control of limits and levels of exposure to consolidated market risk by risk factors or modules, as applicable.

D. Consider the entity's strategy and risk appetite, general transaction practices, and the conditions of the economies and markets in which the entity operates.

E. Implement mechanisms to record orders and transactions made by telephone or any other communication system. These transactions must be supported by prior compliance with existing legal requirements. In any case, within the trading area, the entity must not allow the use of cell phones, cordless phones, mobile phones, or any other communication equipment or system that does not allow for the recording and/or review of calls and messages sent and/or received to verify the transaction and its terms.

F. Implement the proper and individual recording of orders and transactions carried out by the entity, including the terms and conditions of the transaction, such as the time of the transaction, the counterparty (provided the securities trading system allows it), the amount, the agreed-upon rate, and the term, among others. The entity must retain the corresponding records for the periods generally established by law.

G. Record all telephone communications and maintain a reliable record of data messages used for securities and foreign exchange brokerage operations, as well as for operations with derivative financial instruments and structured products in the front, middle and back office, in order to ensure that all transactions carried out on own account or on behalf of third parties can be reconstructed from the moment the purchase or sale orders are issued, their execution and their corresponding clearing and settlement, in accordance with current rules.

H. Ensure strict organizational and functional independence between areas that carry out

operations on behalf of third parties, those that manage third-party portfolios, those that manage collective investment funds and, in general, ensure independence between authorized activities when this has been provided for in the applicable regulations.

1.2.1.4. Monitoring

Market risk control will allow the Entity to continuously monitor the evolution of its exposure to market risk and must correspond to the volume and complexity of the Entity's operations. The monitoring activities planned by the Risk Unit for compliance with market risk control are as follows:

A. Monitoring of Limit Consumption: Market risk exposure levels and limits established by the Board of Directors must be monitored daily and reported to the Legal Representative and the Treasurer. This monitoring must include consolidated market risk exposure levels by risk factor or module.

B. Monitor and report results: the quantification of the impact of market risk should be included in the P&L (Profit and Loss Statement).

C. Monitor counterparty quotas: Additionally, the quotas authorized to operate in the securities market must be monitored to determine the Entity's trading profile and the business carried out under clean market conditions.

D. Reports to the Risk Committee: The risk management area must periodically report to the Risk Committee on the results of invested resources, the status of limits, and the risk assumed in operations relative to the profit obtained. This aims to create information channels within the Entity, where the Risk Management System (SARM) plays a more significant role in investment decision-making.

E. Monthly reports to the Board of Directors: The market risk department must prepare a comprehensive monthly report on the status of the SARM for the Board of Directors. This report must, at a minimum, include the status of the limits, market conditions, and compliance with trading limits.

F. Market monitoring: Monitoring market conditions through technical and fundamental analyses of assets and issuers complements the identification of potential threats that could affect managed investments. The Risk Unit periodically analyses market information and conducts stress tests to identify the most critical factors in portfolio management. These stress tests are presented to the Risk Committee.

1.2.2. Boundaries

The Entity has established criteria for defining loss limits and maximum levels of exposure to market risk, as well as limits for positions at risk according to the type of risk, business, counterparty, or product.

This is in accordance with the Entity's business plan and MAR (Market Risk Assessment) and the economic and market environments in which it operates.

The limits that the Entity establishes for its exposures in treasury activities must comply with the following requirements:

A. Establish the parameters for defining special limits at the trader, trading desk and product level, according to the structure, characteristics and operations authorized for each type of entity.

B. Establish it individually, leaving its aggregation or global calculation planned at least once a day.

C. Be consistent with the entity's risk level.

D. Include market risk exposure levels so that they can be reviewed periodically to incorporate changes in market conditions or new decisions resulting from risk analysis.

E. Establish guidelines to ensure that all transactions are recorded promptly so that effective control of compliance with limits can be carried out.

F. Establish mechanisms to ensure that the limits are known in a timely manner by the officials in charge of the negotiations and by the traders.

G. Establish mechanisms to ensure that compliance with the limits is monitored by functional areas other than those responsible for negotiations.

1.2.2.1. Policy on the Estimation of Economic Capital

The Entity's methodology for estimating the necessary capital levels to absorb losses arising from exposure to market risks, thereby adequately protecting its equity, consists of continuously monitoring the solvency ratio limit established by law at 9%. This allows the Entity to determine its capacity to assume different risks and absorb or withstand the resulting losses. Additionally, for the other lines of business, the methodology includes monitoring the minimum capital required to operate each of them.

1.3. Disclosure of information and reports

The Entity will implement an effective, truthful, efficient and timely reporting system, both internal and external, that will guarantee the functioning of its procedures and compliance with regulatory requirements.

Market risk management involves establishing a set of risk level reporting policies. These policies can be internal, within the organizational structure itself, or external, to meet the requirements of regulatory bodies and other stakeholders. They define the communication channels, the means used, and the

established frequency.

In communicating market risk monitoring, there are defined channels as follows:

1.3.1. Internal Disclosure

As a result of monitoring, the Risk Unit must prepare semi-annual reports that establish the entity's risk profile. The Entity's Legal Representative, in their management report to the General Shareholders' Meeting at the close of each fiscal year, must include an indication of the actions taken regarding market risk management.

The Risk Unit is also responsible for preparing reports on compliance with policies, limits, and risk exposure levels for market risk, for presentation to the Legal Representative and the Board of Directors. These reports are presented in an understandable manner and show exposures by risk type, business area, and portfolio. They also indicate the established limits, the degree of compliance, and the quantification of the effects of positions on profits, equity, and the Entity's risk profile.

Within the Entity, three circuits of regular information on market risks are distinguished: i) within the Treasury itself, ii) between the Risk Unit and the Treasury, and between the Risk Unit and the main administrative, management and leadership bodies of the Entity.

1.3.2. External Disclosure

AIAC will provide the public with the necessary information so that the market can assess the market risk management strategies adopted by the Entity. The characteristics of the disclosed information will be related to the volume, complexity, and risk profile of the Entity's operations. This information must include the business objectives, strategies, and risk-taking philosophy. AIAC's risk management reporting policies must consider its external reporting obligations and the desirability of increasing transparency in the information provided to market participants.

The risk measurement tools used in AIAC, and the details of information they provide, must allow compliance with information requirements and, specifically, must be able to satisfy the information requested by the SFC or AMV, shareholders, among others.

1.3.2.1. Reports on Market Risk Measurement

The results of the market risk measurement will be reported to the SFC with the established periodicity in the formats provided for that purpose.

Additionally, the value at risk of the managed portfolios must be reported through the technical data sheet or similar document; this value at risk must be obtained through the calculation of the SFC standard model defined in Chapter XXXI of the CBCF.

1.3.2.2. Reports on portfolio formation

In accordance with current instructions, the Entity will report to the SFC information on the composition of its investment portfolios, investment updates and treasury operations.

1.4. Documentation

AIAC will maintain the documentation necessary to support the proper management of market risk, such documentation will comprise at least:

A. The operating manuals for the front office, middle office, and back office.

B. The entity's Code of Ethics.

C. Documents and records that demonstrate the timely, effective, and efficient operation of Market Risk Management.

D. The reports from the Board of Directors, the Legal Representative, the Risk Unit, the Risk Committee, and the control bodies.

E. The minutes of the Risk Committee, the Audit Committee, and the reports to the Board of Directors and the Legal Representative.

F. All transactions that generate trading positions must be recorded by the accounting department in a timely manner.

G. Methodologies for valuing financial instruments and measuring risks.

H. Reports prepared by the Risk Unit on compliance with limits and the level of exposure to market risk and associated risks.

I. The procedure to follow in case of non-compliance with the established limits.

2. OPERATIONAL RISK MANAGEMENT

2.1. Definition of operational risk

It is the possibility of incurring losses due to deficiencies, failures, or inadequacies in human resources, processes, technology, infrastructure, or due to the occurrence of external events. This definition includes legal and reputational risk associated with such factors.

Legal Risk (RLG): It is the possibility of loss that an Entity incurs when it is sanctioned or obliged to compensate for damages because of non-compliance with rules or regulations and contractual obligations.

Legal risk also arises from breaches in contracts and transactions, resulting from malicious acts, negligence, or unintentional acts that affect the formalization or execution of contracts or transactions. This applies to all activities and includes third parties acting on behalf of the entity with respect to outsourced processes and/or activities.

Additionally, for the purposes of operational risk management, the following definitions should be considered:

A. Losses: Economic quantification of the occurrence of an operational risk event, as well as the expenses derived from addressing it.

B. Gross Loss: This refers to the loss before any recoveries.

C. Net Loss: This is understood as the loss after considering the effects of recoveries. A recovery is a separate event, related to the gross loss, which does not necessarily occur in the same period in which funds or economic flows are received.

2.2. Components

2.2.1. Stages

2.2.1.1. ID

To properly identify the entity's operational risks, it is necessary to document and identify processes and their activities and establish identification methodologies to determine the operational risks of each process. Based on these methodologies, identify potential and actual operational risks in each process. Additionally, the entity's process documentation will be available, providing information on inputs, activities, and outputs, thus facilitating the identification of operational risks.

AIAC will have clear documentation of each of the processes, carrying out the identification of potential and actual operational risks associated with each of the activities, which form the Entity's Risk and Control Matrix.

For risk identification, the primary criterion will be the input of those responsible for the processes, and especially the staff involved in the operation of the respective processes. Workshops will be conducted to encourage participant engagement and commitment to risk management and control. This methodology is also valid for the other stages of risk analysis and management, as it is based on the principle of communication and consultation as the foundation for gathering diverse perspectives on risks.

Risk identification is represented in risk maps. These maps are a visual representation or description of the various aspects considered in the risk assessment. Risk maps are created using procedure diagrams developed for a specific process, linking each of its basic activities.

The Risk Unit and the process owner or manager analyse each activity within the specific process to identify the operational risks associated with it. These operational risks can be identified as either potential risks (those that have not yet occurred but could) or known risks that have occurred in the past within the organization.

The identification stage must be carried out prior to the implementation or modification of any process, product, service or channel, as well as in cases of merger, acquisition, transfer of assets, liabilities and contracts, among others.

The following criteria are considered for risk identification:

A. Internal factors

   a. Processes: It is the set of activities that are interrelated with each other for the transformation of input elements into products or services and that seek to satisfy a need.

   b. Technology: This refers to the set of tools used to support the entity's processes. This includes hardware, software, and telecommunications elements.

   c. Infrastructure: This refers to the set of support elements necessary for the operation of an organization. These include buildings, workspaces, storage, and transportation.

   d. Human Resources: This refers to all individuals directly or indirectly involved in the execution of the entity's processes. For the purposes of this Chapter, a direct relationship is defined as one based on an employment contract in accordance with current legislation, while an indirect relationship encompasses any legal arrangement for the provision of services other than one based on an employment contract.

B. External factors

a. These are situations associated with the force of nature or caused by third parties, which escape the control of the entity in terms of their cause and origin.

2.2.1.2. Measurement

The Entity will measure the probability of occurrence of the identified operational risks, and their impact should they materialize. This measurement must be qualitative and, when historical data is available, quantitative. A minimum time horizon of one year will be considered for determining the probability of occurrence.

At this stage, the Entity must determine existing controls and analyse risks in terms of probability and impact within the context of those controls. The analysis should consider the range of potential consequences and whether those consequences are likely to occur.

To perform an adequate risk analysis, it is important to know the level of effectiveness of existing controls and thus establish the residual risk, that is, the risk that remains after applying the control activities implemented in the company.

Risk Levels	Description
Low	The occurrence of the event does not imply significant severity and does not destabilize the organization. Therefore, it does not warrant the investment of additional resources or time beyond those already applied to its management. It can be managed through routine procedures.
Half	Should this occur, it would cause moderate consequences that do not exceed the organization's tolerance level. It requires attention from the Operational Risk Unit and the relevant Management. It should be managed with additional controls to be implemented in the medium term or by strengthening existing ones.
High	The risks located in this region require the development of priority actions in the short term for their management due to the high financial, legal, reputational or operational impact that they could cause if they occur.
Extreme	This event could affect the stability of the Entity. It requires priority measures and the immediate attention of Senior Management.

The meaning of the risk levels, estimated by qualitative methods, is as follows:

The analysis should consider the range of potential impacts and whether these impacts are likely to occur, for which quantitative and/or qualitative measurement techniques are usually used, as shown below:

Operational risk probability table

Assigned rating	Criterion
1 Rare	There is a very low probability that the event will occur within the specified time. It will occur less than once a year on average.
2 Eventually	Low probability of the event occurring within the specified time. It will occur at least once a year on average.
3. It Can Happen	There is a moderate chance that the event will occur within the specified time. It will occur at least once every six months on average.
4 Likely	High probability of the event occurring within the specified time. It will occur at least once per quarter on average.
5 Very Frequent	There is a very high probability that the event will occur within the specified time. It will occur at least once a month on average.

Operational Risk Impact Table

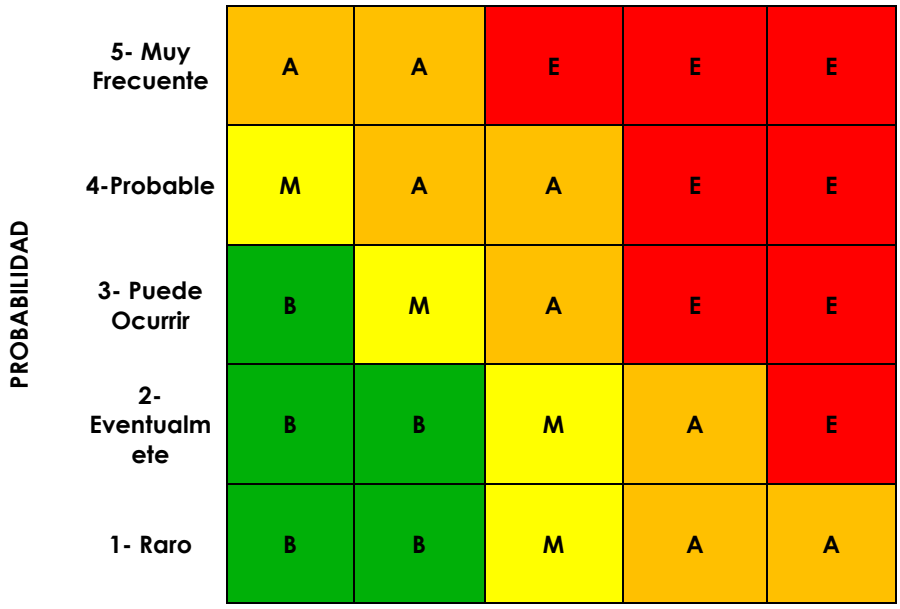
Assigned rating	***Economic***	***Legal***	***Operational***	***Reputational***
Reducer Description	*Financial losses could occur due to the materialization of the risk, as follows:*	*What legal implications could this risk have?*	*The level of reprocessing of activities generated by the risk could be:*	*The risk can generate a negative image in the following ways*
1 Insignificant	From 0 to $1 MM	It does not generate recommendations from a regulatory body	Less than 10%	It does not affect the Entity's image in the market
2 Minor	From $1 million to $20 million	Recommendations issued by a control or oversight body	Between 11% and 25%	Negative situations that do not reach the mass media
3 Moderate	Losses of $20 million to $50 million	Disciplinary proceedings or statement of charges issued by a control or	Between 26% and 35%	Negative information in low-circulation media outlets

Assigned rating	Economic	Legal	Operational	Reputational
		oversight body		
4 Mayor	Losses of $50 million to $200 million	Sanctions and Fines by a regulatory body	Between 36% and 49%	Negative comments from customers, suppliers, or employees in mass media without counterproductive effects
5 High Impact	Losses exceeding $200 million	Intervention by a control body	More than 50%	False information in high-circulation mass media, social networks and news

The impact is rated according to the subjectivity reducers, as follows: Economic, Legal, Reputational and operational.

Subsequently, the controls that mitigate the inherent risks identified according to the defined criteria are considered, and the risk analysis is carried out again in the context of those controls, applying the formula R = P x I (Risk = Probability x Impact) to obtain the Residual Risk profile.

Risk Assessment Standards AS/NZ 4360 (NTC 5254)



2.2.1.3. Control

This stage aims to establish the measures used to control the identified inherent risks, thereby mitigating their impact or reducing their probability of occurrence should they materialize. The goal is to increase the likelihood that the process or subprocess will meet workflow requirements and achieve its goals and objectives. This stage of the model determines the entity's residual risk profile.

A control is any measure taken to detect or reduce the probability of occurrence and/or the magnitude of impact should a risk materialize. Controls are incorporated into processes to ensure that workflow requirements and overall service objectives are met.

To carry out this stage, an inventory of controls will be made, including their respective description and assessment, to obtain the residual risk assessment, which will allow identifying the modification that took place for the risks.

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

A. Sufficient: prepare the appropriate quantity.

B. Understandable: simple and clear.

C. Economic: the aim will be to ensure that the cost is lower than the benefit.

D. Effective, that is, that they are both effective (allowing the detection of risk and reducing the probability of occurrence or impact) and efficient (correct use of resources for their application).

E. Timely: existing when required.

Immersed in the processes: it assumes that carrying out the activities includes control.
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 that will allow us to determine if it is well designed or if it should be redesigned.

Criterion	Description.
Type of Control	• **Preventive:** Preventive controls provide the first line of defence or barrier against threats that could affect an organization's assets. They constitute the outermost security ring, stopping most threats; they neutralize (block) the agents that generate them or eliminate vulnerabilities. These controls are action guidelines or parameters to ensure that activities are carried out in a predetermined, safe, and efficient manner. • **Detective:** These are designed to detect the presence of a generating agent. They are alarms that are triggered to indicate deviations from what "should be." • **Corrective:** The purpose of these controls is to take action to correct the impact of the materialized risk.
Control Class	• **Manual:** The control is carried out by a person without the use of any technological tool. • **Semi-automatic:** The control execution requires a technological tool and the intervention of a person. • **Automatic:** The control is executed by a technological tool without the need for human intervention.
Periodicity	This field evaluates the frequency with which the control is executed in the process.
Responsible	The person responsible for carrying out the control within the process is determined.
Documentation	It is specified whether the control is fully documented, partially documented, or not documented at all.
Evidence	It is noted whether evidence of the execution of the control is preserved.

Based on the above, the Entity determines the net operational risk profile.

2.2.1.3.1. Outsourcing

AIAC may contract with individuals and/or legal entities for the development of its processes through outsourcing, if this does not involve the delegation of professional expertise. In any case, AIAC must: (i) conduct a risk analysis to determine the processes and/or activities to be outsourced; (ii) understand the operational risk associated with the outsourced processes and/or activities; (iii) have effective policies in place to incorporate risks arising from outsourcing into its risk strategy; and (iv) identify the critical processes and/or activities within the outsourced processes and/or activities.

Regarding processes and/or activities identified as critical to the entity, the following minimum requirements must be met:

A. Define the criteria and procedures from which the third parties will be selected.

B. Include in contracts entered with third parties, or in those that are extended from the date of this chapter's entry into force, at least the following aspects:

   a) Obligations of the parties.

   b) Service levels.

   c) Operation in contingent situations.

   d) Management of operational risks that may affect the fulfilment of the third party's obligations.

C. Confidentiality agreements regarding the information handled and the activities carried out.

D. Manage the risks arising from the provision of the service by the third party, particularly when it serves several entities.

E. Having the necessary procedures in place to verify compliance with obligations by the third party.

F. Include outsourced activities within the scope of the assessments carried out by the risk management function and internal audit.

2.2.1.3.2. Business continuity plan

AIAC defines and implements a process to manage business continuity called the Business Continuity Plan (BCP), and for its compliance, the Board of Directors will oversee developing contingencies that guarantee the internal and external functioning of events that occur that affect business continuity, as well as carrying out tests and keeping said plan updated.

AIAC's PCN takes as a reference the ISO 22301 standard, this normative standard will allow the Entity

to maintain adequate management of the risks generated by the unavailability of services in disaster scenarios.

The strategies implemented by PCN have the fundamental objective of addressing crisis management and subsequent recovery of critical activities affected by an exceptional situation, having previously prepared all the organizational and material means necessary for that recovery.

The Business Continuity Plan (BCP) includes elements such as emergency prevention and response, crisis management, contingency plans, and the ability to return to normal operations. The BCP meets the following requirements:

A. Having passed the necessary tests to confirm its effectiveness and efficiency.

B. To be known by all interested parties.

C. Cover at least the identification of risks that may affect the operation, the activities to be carried out when failures occur, operating alternatives and return to normal activity.

The responsibilities inherent in ensuring continuity require the active participation of various functions. This involves all officials by generating a culture of continuity within the organization, so that they can face events calmly and professionally, and plan accordingly to carry out their assigned actions, allowing the Entity to survive the planned risk event.

Under this framework, the Technology process is responsible for ensuring that there are contingency plans whose primary objective is to prevent and, if necessary, solve the problems, failures and incidents that may occur in any of the processing and storage devices that make up the comprehensive information management and processing system.

Both the Risk Unit and the Technology area must ensure that the contingency and continuity policies defined by the Entity are complied with internally, as well as by third parties that support the fulfilment of AIAC's corporate purpose.

2.2.1.4. **Monitoring**

The primary purpose of monitoring activities is to verify and evaluate the effectiveness of the processes linked to the Operational Risk Management System. Monitoring should help identify whether the measures adopted by the Entity meet its operational risk management needs and allow for changes and modifications to be made if necessary.

This process must be carried out not only by the system administrator but must also be accompanied by the internal control bodies of the Entity, who must issue opinions about the implementation of the system and give recommendations that allow strengthening it through the improvement of the

deficiencies evidenced during these reviews.

The results of the inherent and residual risk profiles must be made known to the Legal Representative, the Risk Committee, the Audit Committee and the Board of Directors for their respective follow-up.

Monitoring must be carried out through an effective tracking process that facilitates the rapid detection and correction of deficiencies in the SARO (System for the Analysis of Risk and Risk). The frequency of monitoring must be appropriate to both potential and actual events, and in any case, at least a minimum frequency of six months must be guaranteed.

The monitoring of the SARO (System for the Analysis of Risk Assessment) must ensure that controls are functioning in a timely and effective manner. Likewise, it must ensure that residual risks are within the acceptable levels established by the Entity.

Monitoring should identify elements that threaten the effectiveness of the SARO and opportunities for improvement to address them. Monitoring activities should promote the continuous improvement of the SARO.

The activities for carrying out the monitoring stage are:

A. Periodic Monitoring of Risk Profiles and Exposure to Loss Situations.

B. This will ensure continuity in the action plans defined for risk events and verify that these plans are effectively implemented as established.

C. Ensure periodic monitoring of the Entity's level of risk exposure.

D. Implement effective monitoring that allows for the detection and correction of deficiencies found at least every six months.

E. Monitor the behaviour of the defined indicators.

F. Verify that the controls are functioning in a timely, effective, and efficient manner.

G. Ensure that residual risks are within the acceptance levels established by the Entity.

H. Evaluate the effectiveness and compliance with the requirements in the operational risk event log and verify that it is properly updated.

I. Evaluate the procedures for recording operational risk, analysing the accounting and economic impact that such events have on the Entity.

J. Perform ongoing monitoring of records, procedures, and any modifications that may arise during

the implementation and start-up of risk management.

K. Submit periodic reports on the operation and development of risk management, analysing in detail each relevant finding, and making the respective recommendation.

L. Evaluate whether the corrective measures established by the Risk Unit and the process owner are effectively implemented to reduce operational risk events that occur.

2.2.1.4.1. Monitoring of Risk Treatment Plans

Action plans or risk treatment should be monitored for threats that have a Residual Risk above the acceptable level (existing protection other than Appropriate and Residual Risk other than Low).

These monitoring tasks should be implemented through:

A. Indicators: Descriptive and prospective indicators must be designed, which must be calculated and reported by the Operational Risk Unit; these correspond to formulas that reflect whether risk control and contingency plans are adequate or not.

B. Control indicators: Number of times the control was applied over the number of associated risk events detected.

C. Performance indicators: Number of events that occurred out of total operations.

D. Loss Report Evaluation: This allows for the analysis of operational risks using a quantitative methodology. As these reports are implemented, their analysis will allow for the evaluation of the frequency and impact of identified risks and will form the basis for measuring control indicators to set achievable goals.

E. Changes in the structure of processes: Through the periodic review of procedures and the verification of compliance with the manuals that govern their implementation, the response that will be necessary to implement because of the implemented modifications must be analysed.

F. Launch of new products and services: As a requirement for any modification or implementation of a new process in any area of the Entity, it must be subject to the previous analysis through workshops or working meetings, to evaluate the inherent risk and the controls that must be implemented, so that, through the Operational Risk Unit, the respective report is presented to the Board of Directors.

G. Changes in the regulatory framework: Verifying that internal rules and procedures correspond to the modifications made in laws and documentation issued by supervisory bodies.

H. It will also be necessary to analyse whether the modifications comply with all control activities

regarding the execution of the processes involved.

I. Changes in risk exposure: These may arise from situations inherent to the dynamics of the Entity's management. The need to adjust control procedures will be verified to ensure they reduce risk to levels acceptable within the AIAC structure.

2.2.2. Training

2.2.2.1. Training Policies

A. AIAC must design, schedule and coordinate training plans on the SARO aimed at all officials; their contents will be designed according to the process to which they belong.

B. Training programs should be conducted on an annual basis.

C. Training programs must be provided during the induction process of new officials and third parties whenever there is a contractual relationship with them, and they perform functions of the entity.

D. Training programs must be constantly reviewed and updated in accordance with any changes that may occur in current regulations or applied methodologies.

E. Training programs must have mechanisms for evaluating the results obtained to determine the effectiveness of these programs and the achievement of the proposed objectives.

2.2.2.2. Training Strategies

Operational risk training is mandatory for all Entity personnel. The depth, content, and scope of this training will vary, adapting to the different stakeholder groups and their specific needs.

A. New staff: The Operational Risk Unit will conduct SARO training as part of the staff induction program.

B. Current Officials: The Operational Risk Unit will conduct annual internal SARO training for all officials and areas of the Entity. SARO and its elements will also be disseminated through the intranet, and periodic evaluations will be established to certify knowledge of the system.

2.3. Special rules regarding seizure orders

Although the Entity does not offer products or services that are subject to seizure, in accordance with the National Political Constitution, both individuals and authorities must act in good faith, respect the authorities, and cooperate with the justice system. In this regard, the information requested by judicial and administrative authorities from supervised entities is confidential and private and is subject to the purposes of administering justice and the investigations carried out by said authorities.

Therefore, in compliance with the regulatory framework regarding attachment orders from judicial and administrative authorities contained in articles 593 and 594 of Law 1564 of 2012 (General Code of Procedure), numeral 5.1. of Chapter I, Title IV, Part I of the Basic Legal Circular, the Tax Statute and other related regulations, the Entity has developed the following mechanism for handling attachment orders.

2.3.1. Reception

The Entity may receive garnishment orders through the authorized communication channels, which are:

Physical Address	Carrera 7 No. 75-66 Floor 7 Office 702
Email	i. Legal Representation: Felipe.gomezbridge@AIACgroup.com.co Sebastian.gallego@AIACgroup.com.co ii. Legal and Compliance Department: Monica.rohenes@AIACgroup.com.co iii. Risk Management: Daniela.guzman@AIACgroup.com.co
Web page	https://www. AIACgroup.com/es-co-aiac/pqrs-peticiones-complaints-claims-and-suggestions / **pqrsfiduciaria@AIACgroup.com.co**

2.3.2. Prosecution

Once the Entity receives the seizure orders, they will be processed as follows:

Physical Address	i. The general reception of the building where the offices are located will be responsible for immediately informing the Entity 's reception about pending courier service for face-to-face attention. ii. Once the Entity has been informed of the receipt, it will be responsible for

	authorizing access to the Entity 's facilities for the courier service used by the judicial or administrative authority. iii. Once at the Entity 's offices, the administrative assistant will receive and stamp the copy of the document as received. The stamp must include the date the document was received. iv. The documents received will be immediately handed over to the Legal and Compliance Department so that it can then carry out the necessary legal procedures and take the appropriate measures.
Email	Entity 's officials must immediately forward the communications received to the Entity 's Legal and Compliance Directorate so that it, in turn, can carry out the legal procedures and implement the measures that may be necessary.
Web page	Entity 's website has provided a link for sending direct communications to the email: **pqrsfiduciaria@AIACgroup.com.co , which is managed by the** Entity 's Legal and Compliance Department . Once the communications are received, the Entity 's Legal and Compliance Department will be responsible for carrying out the legal procedures and taking the necessary measures.

2.3.3. Attention and Timely Response

The Legal and Compliance Department will be responsible for:

A. Verify whether the natural or legal person referenced in the seizure order corresponds to a client of the Entity.

B. In case of doubt regarding the identity of the natural or legal person on whom the seizure order is issued, the Entity that decrees the seizure must be consulted immediately so that it can define or clarify the identity of the person in question.

C. If the client is NOT linked to the Entity, this circumstance must be reported to the jurisdictional or administrative authority that decrees the seizure order.

D. If the client is linked to the Entity, the Legal and Compliance Department must:

E. Identify the non-sizeable status of the resources.

F. Ensure compliance with the limits of non-seizure indicated in the applicable regulations, as well as the limits of the measures, without exceeding the amounts of the seizures ordered by the judicial or administrative authorities.

G. Draft the response to the request for review and consideration by the Entity's Management.

H. Once approved and signed by the Entity's Legal Representative, it will be sent to the corresponding judicial or administrative authority, through the channel provided by them.

I. To issue the necessary internal orders to block/deposit the resources determined by the competent judicial or administrative authority in compliance with the order received.

2.3.4. Compliance

A. Account impact: The Entity must affect the deposits for the corresponding value according to the records presented in the attachment order in accordance with Art. 1387 of the Commercial Code and numerals 4 and 10 of Art. 593 of the General Code of Procedure.

B. Information on the amount affected: The Entity must provide the client with supporting documentation showing the amount affected by the order, indicating that the seizure is provisional.

C. Deadline for depositing the seized sums: Within 3 days following the notification of the seizure, the Entity must deposit the sums retained in the judicial deposit account, and inform the court definitively about the total amount of the seized sum, sending it the receipt stating that said value is at its disposal in the "judicial deposit account", in accordance with the provisions of Decree 2419 of 1999.

D. Procedure regarding amounts deposited after the seizure order: If the balance in the product on the date and time the seizure order is communicated is less than the amount indicated in the document, the amounts deposited subsequently are affected by said order until the limit established therein is covered.

E. Procedure when the seized balance is less than the limit indicated in the order: When the seized balance is less than the limit indicated in the court order, the Entity cannot allow the

disbursement of funds.

F. Procedure in case of precautionary measures decreed on non-sizeable resources: In accordance with the provisions of articles 48 and 63 of the Political Constitution, 134 and 182 of Law 100 of 1993, 19 of Extraordinary Decree 111 of 1996 (Organic Budget Statute), 91 of Law 715 of 2001, 8 of Decree 050 of 2003, the following resources are non-sizeable: the Social Security System, the revenues incorporated into the General Budget of the Nation as well as the assets and rights of the bodies that make it up, the General System of Participations -SGP-, Royalties and other resources to which the law grants the status of non-sizeable.

G. If the Entity receives any attachment order related to the resources, it must follow the rules established in Article 594 of the General Code of Procedure.

H. Procedure in case of precautionary measures decreed by territorial entities in coercive collection processes of tax debts: In accordance with the provisions of Articles 5 of Law 1066 of 2006 and 823 of the Tax Code, in the case of precautionary measures decreed by territorial entities in coercive collection processes of tax debts, the procedure indicated in paragraph 5 of Art. 837-1 of the Tax Code must be complied with, until the lawsuit filed against the tax acts that serve as an executive title is admitted or the defendant guarantees the payment of 100% of the value in question, through a bank guarantee or insurance company guarantee.

2.3.5. Preservation and Archiving of Information

The Entity will keep the files and documents related to these orders and their management, in accordance with article 96 of the Organic Statute of the Financial System (EOSF), for a period equivalent to 5 years counted from the date of the last entry, document or voucher, and may use for this purpose, its preservation on paper or in any technical, magnetic or electronic means that guarantees its exact reproduction.

3. LIQUIDITY RISK MANAGEMENT

3.1. Definition of liquidity risk

Liquidity risk is understood as the contingency of not being able to fully, promptly, and efficiently meet expected and unexpected cash flows, both current and future, without affecting the course of daily operations or the entity's financial condition. This contingency (funding liquidity risk) manifests itself in the insufficiency of available liquid assets and/or the need to assume unusual funding costs. In turn, the entity's ability to create or unwind financial positions at market prices is limited either because the market lacks adequate depth or because of drastic changes in rates and prices (market liquidity risk).

Liquidity risk is also a perception risk and almost always residual. Hence the importance of designing a liquidity risk management system (LRMS) that is integrated with the management of other risks that directly or indirectly affect the liquidity risk management strategy.

3.2. Components

3.2.1. Stages

3.2.1.1. ID

The Entity is a Trust Company that will primarily engage in investment trust activities and, in this capacity, will execute fiduciary assignments (“Fiduciary Assignments”) or commercial trusts (“Commercial Trusts”), with the objective of discretionarily managing clients' portfolios and acting as the principal of their funds. It should be noted that, as a matter of internal policy, the Entity will not conduct proprietary trading.

Therefore, the SARL allows for defining and identifying the liquidity risk to which the Entity is exposed based on the type of positions assumed and the products and markets it serves, in accordance with the operations authorized as a Trust Company. This must be done at both the individual and financial conglomerate levels (if applicable).

Risk identification will be carried out in a preliminary phase of analysis and implementation of the processes necessary for the negotiation of a new product. This process will be carried out through the Risk Committee, where the risk profile will be determined and the impact that these new products have on the total risk profile, equity, and profits will be quantified.

This implies that before negotiations with new products begin, there must be adequate knowledge of all aspects of the product, and the risk profile must be identified and the impact of these on the entity's level of exposure to liquidity risk, as well as aspects related to their valuation and accounting, must be quantified.

All operations implemented as a new product must be previously reported to the Risk Committee for recommendation to the Board of Directors, who is responsible for their final approval.

3.2.1.2. Measurement

This stage allows quantifying the minimum level of liquid assets, in national and foreign currency, that must be maintained daily to prevent the materialization of liquidity risk; that is, it allows the Entity, at least, to meet its payment obligations in a timely and complete manner.

The Entity must establish the conditions, type of operations and limits for the provision of and access to liquidity within the financial conglomerate and from the Entity to related parties, which mitigate the risk of contagion in crisis conditions.

The Entity will have a proactive and forward-looking approach to identify funding mismatches across various time horizons and to analyse the emerging market liquidity risk of the investment portfolio, enabling it to create early warning signals and establish limits aimed at preventing the materialization

of risks in the presence of adverse market events, within the entity or both, in terms of liquidity.

Likewise, the Entity will be able to measure and project the cash flows of its assets, liabilities, and off-balance sheet positions over different time horizons, both in a normal scenario and in an adverse one, in which cash flows deviate significantly from what is expected, due to unforeseen changes in the market environments, the Entity, or both.

3.2.1.2.1. Methodology for Measuring Liquidity Risk

Regardless of the measurement model used, it is the Entity's duty, for the purposes of its risk management, to anticipate the potential scenarios that will test its ability to generate sufficient liquid resources to address a liquidity crisis.

The Entity will design and implement internal methodologies for measuring liquidity risk arising from transactions carried out on behalf of third parties; this includes designing a Liquidity Risk Indicator and establishing prudential limits for this indicator, which AIAC is obligated to comply with. As a matter of internal policy, the Entity will not conduct transactions on its own behalf.

These models will be designed considering the nature, line of business or significant activity and authorized operations, and must meet the minimum requirements set forth in subparagraph 5.3.1.2.2 of Part II of Chapter XXXI of the CBCF. The results obtained and, in general, all documentation on the parameters, assumptions, construction, and operation of the internal model will be made available to the SFC.

In any case, for the purposes of homogeneous and permanent monitoring by the SFC of the main variables related to liquidity and the Entity's exposure to liquidity risk under different scenarios, the Entity will perform the liquidity risk measurement daily and report this information weekly in accordance with the instructions indicated in Annex 1 of Chapter XXXI of the CBCF, in the corresponding format that the SFC adopts for this purpose.

While the results obtained from the SFC standard imply moderately stressed performance parameters, they do not exempt the Entity from the obligation to carry out the appropriate process for measuring and evaluating exposure to liquidity risk specific to its operations, nor do they constitute a guide for managing stress situations or daily liquidity. The established indicators and limits are only one component of the obligations arising from the adoption of the SARL (Liquidity Risk Assessment System) contained in the regulations, under which it is the Entity's sole responsibility to carry out effective, efficient, and timely management of such risk, and in particular, to anticipate and address potential events that generate exposure to liquidity risk.

3.2.1.2.2. Liquidity Risk Indicator Limit – LRI

Regardless of the measurement model used by the Entity for daily reporting, the accumulated Liquidity Risk Indicator (LRI) for the horizons of one (1) and seven (7) calendar days must always be equal to or

greater than zero (0) –LRIm, and greater than or equal to 100% in the case of the ratio –LRIr–.

3.2.1.2.3. Significant Exposure to Liquidity Risk

The Entity is considered to have a significant exposure to liquidity risk when in each report the Liquidity Risk Indicator -IRLm- for one (1) day or seven (7) days, is negative.

3.2.1.2.4. Performance tests

The purpose of internal model performance testing is to determine the consistency and reliability of the estimated liquidity risk models and indicators. This testing essentially consists of an ongoing review process by the Entity of the internal model used and the validation of the assumptions, parameters, and expert judgments underlying the liquidity risk indicator calculation. When the Entity estimates model parameters using statistical processes, performance testing requires the Entity to compare, also based on statistical tests, the projections of these parameters with the actual ex-post values verified during the relevant period and make any necessary adjustments to the model.

Performance tests will be conducted at least once a month. The test results and the methodology used by the Entity for conducting them will be documented and available to the SFC upon request.

3.2.1.2.5. Stress tests

The Entity must conduct stress tests to assess its resilience to adverse scenarios that could affect its liquidity and that of the system. This assessment should be based on identifying liquidity levels and mismatches across different time horizons and quantifying exposures to future liquidity crises and their impact on the Entity's cash flows, profitability, and solvency, as applicable. This analysis must meet the following criteria:

A. This analysis should be conducted at the business line level, both individually and on a consolidated basis. It should also include the potential response and impact of other market participants relevant to the entity.

B. The models designed and implemented for the development of the tests must correspond to the size, complexity, systemic importance, profile and risk appetite of the entity, as well as be statistically robust and constitute an input in decision-making on risk management and in the development of the contingency plan.

C. The frequency of stress tests, their review, and updates depend on the size of the entity, its relative importance within the system, and its level of exposure to liquidity risk. This frequency must be at least quarterly. The entity must be able to increase the frequency of tests under special scenarios such as changes in market conditions, crises, or at the request of the SFC (Superintendency of Finance).

D. The tests must consider scenarios with varying levels of severity (medium, high, and extreme), which must include at least situations such as economic slowdown, concentration in assets and liabilities, expansion of interest rate margins in the secondary market, increase in funding costs, decrease in credit rating, decrease in available funding sources, increase in early withdrawals, increase in delinquency indicators, additional collateral requirements for money market operations, and reputational risk situations.

The results of the stress tests in each scenario will serve to generate indicators that activate the corresponding contingency plan.

The assumptions, parameters, analysis, measurement, and results of these tests will be documented and available to the SFC.

3.2.1.3. Prudential Measures to Counteract Significant Exposure to Liquidity Risk

When the Entity notices that its IRL is negative regardless of the measurement model used, the Entity's Legal Representative must immediately inform the SFC in writing about:

A. The fundamental reasons that, according to this analysis, caused the IRL to fall to 1 or 7 days below the established limit,

B. The temporary or lasting nature of such a situation, and

C. The adjustment plan containing the actions and/or measures that the Entity will adopt to restore the IRLr to 110% within a period of no more than five (5) business days.

3.2.1.4. Corrective Measures to Counteract Significant Exposure to Liquidity Risk If the Entity presents any of the following situations:

A. He did not submit an adjustment plan in the terms described above,

B. The adjustment plan was objected to by the SFC,

C. The precautionary measures outlined in that plan were not followed.

D. The implementation of the adjustment plan did not allow the IRLra to be restored to 110% within the established five (5) business days, or

E. If, for the third time in a 30-day period, the company presents an adjustment plan, it will not be able to acquire new clients.

If one of these situations arises, the Entity may not carry out the operations indicated in Article 5.3.2.4 of Part III of Chapter XXXI of the CBCF. Carrying out any of the operations indicated in the article, under the stated conditions, will be considered an unsafe practice.

Without prejudice to any applicable sanctions, once the Entity restores the IRLr to 110%, it may resume restricted operations.

3.2.1.5. Control

The Risk Unit must take the necessary steps to continuously monitor compliance with the established policies for the proper management of the Entity's liquidity risk and the third-party portfolios it manages. These measures must be approved by and communicated to the Board of Directors and must be proportionate to the volume and complexity of the operations carried out, ensuring a match between the model and the operations performed.

At this stage, the Entity must:

A. To allow the control of exposure levels to liquidity risk and of the general and special limits established by the entity, in accordance with the structure, characteristics and authorized operations.

B. To allow the measurement of liquidity risk, and its incorporation within the entity's risk management and control structure.

C. Consider the entity's strategy and risk appetite, its general transaction practices, and the conditions of the economies and markets in which it operates.

The development of the control will be carried out based on the following activities:

A. Continuously evaluate market conditions so that timely decisions can be made regarding liquidity strategy.

B. Perform the liquidity risk measurement in accordance with the parameters described in this Manual so that the levels of exposure to liquidity risk of both the Entity and the managed portfolios are always known.

C. Prepare reports under normal and stress conditions: daily, the liquidity risk for managed portfolios must be estimated, in addition, market and funding liquidity risk must be monitored daily.

The Risk Unit will propose a scheme of limits and alerts, which will be reviewed annually by the Risk Committee, reporting its follow-up in each of its ordinary sessions.

3.2.1.6. **Monitoring**

It is necessary to evaluate the effectiveness of all stages of the risk management process to make continuous improvements and increase efficiency. Therefore, monitoring activities are established to track the liquidity ratio of the Entity and the portfolios it manages.

In this way, it has been established to carry out periodic reports, among which the daily report that must be presented to the Risk Unit, the Legal Representative and the monthly reports for the Risk Committee and the Board of Directors stand out, in which a summary of the exposure to liquidity risk and compliance with the established limits must be included.

The activities undertaken to monitor liquidity risk will be commensurate with the volume and complexity of the Entity's operations. The reports generated must allow for the evaluation of the Entity's strategies and include a summary of the positions that significantly contribute to this risk.

The guidelines and procedures established for the implementation of this stage must allow the entity to monitor its exposure to liquidity risk.

During this stage, the entity must meet the following minimum requirements:

A. Maintain correspondence with the volume and complexity of the operations carried out by the entity.

B. To allow the monitoring of liquidity risk exposure levels and the general and special limits established by the entity, according to its structure, characteristics and authorized operations.

C. To allow the preparation of management and liquidity risk monitoring reports that evaluate the results of the entity's strategies and include a summary of the positions that contribute significantly to said risk.

D. Implement mechanisms to record and support transactions conducted by telephone or through any other communication system, provided all legal requirements are met. The entity must retain the corresponding records for the periods established by law.

E. Establish the guidelines and policies that the entity must follow for all transactions with related parties that involve liquidity transfers. In fulfilling this obligation, the entity must implement policies and controls for managing liquidity and the flow of resources to and from other companies and/or individuals that are related parties. To this end, the entity must specify in its liquidity risk management strategy its position regarding liquidity transactions and transfers with related parties, as well as the responsibilities it assumes in this area.

F. Consider the entity's strategy and risk appetite and the conditions of the economies and markets in which it operates.

G. Establish that transactions are recorded promptly so that effective control of compliance with limits can be carried out.

3.3. Boundaries

Proper liquidity risk management requires the entity to establish limits consistent with its business plan and risk appetite, including liquidity risk tolerance levels, as well as with the economies and markets in which it operates. Both the limits and tolerance levels should be reviewed periodically to incorporate changes in market conditions or new decisions arising from the entity's risk analysis.

The limits established by the Entity must at least consider:

A. The maximum levels of exposure to liquidity risk, such as concentration levels by term of deposit, depositor, source of funding, issuer, counterparty, economic sector, maturity, type of product and by type of currency, legal and foreign, among others, defined for different time horizons.

B. Maximum exposure levels to day-to-day liquidity risk (including intraday, where relevant) within and between lines of business and entities, under normal conditions. Finally, the definition of these limits should include measures to ensure the Entity's continued operation during adverse market periods, within the Entity, or both.

C. Early warning indicators that allow the identification of increased exposure to liquidity risk or weaknesses in the current position in relation to the following aspects, to the extent applicable:

   a) Rapid asset growth, compared to that of liabilities, or in the face of volatile liabilities.

   b) The growth of concentration in assets or liabilities.

   c) The increase in the outflow of deposits or redemption of term deposits before their maturity.

   d) The decline in the weighted average maturity of liabilities.

   e) Repeated approaches to or breaches of internal or regulatory boundaries.

   f) The significant deterioration of profits, asset quality, and overall financial condition of the entity.

   g) The decrease in the credit rating.

   h) Falling stock prices or rising debt costs.

   i) The increase in funding costs.

j) Counterparties or operations that require additional guarantees or collateral or that resist carrying out new transactions with the entity, elimination or reduction of credit lines and difficulty in accessing long-term sources of financing, among others.

3.4. Liquidity contingency plan

The Entity will have a liquidity contingency plan that allows it to adequately address adverse scenarios in which the Entity must face insufficient levels of liquid assets and manage an increase in exposure to liquidity risk.

The plan must:

A. It should include policies for managing unwanted exposure to liquidity risk and the set of alternative actions to be implemented, as well as the protocols and indicators necessary for their activation. It should also be designed considering the results of stress tests.

B. Be consistent with the complexity of the entity, the risk profile, the scope of operations, and the role within the financial system.

C. The funding contingency plan must explicitly include the strategy for addressing and managing liquidity crises. This plan should outline the policies and procedures for dealing with the unavailability or scarcity of liquid resources during a liquidity stress situation. However, access to the temporary liquidity support provided by the Central Bank should be the last resort in the funding contingency plan, only after all other options have been exhausted, as it is not a committed contingent credit line.

Without prejudice to compliance with the above aspects, the liquidity contingency plan will consider at least the following aspects within the design of the action plan:

A. Access to and availability of funding sources under different adverse scenarios of market stress, increases in transaction costs and asset liquidation, and in guarantee and collateral requirements.

B. The possibility of obtaining liquid resources through money market operations (repos, simultaneous transactions, temporary securities transfers, interbank loans, among others), establishing amounts, guarantees, and counterparties willing to provide the required financing based on the anticipated economic and financial situation. And the possibility of obtaining new liquid resources, whether fresh or through renewals of deposits and/or loans.

C. The transfer and/or sale of investments, loan portfolio or other assets and the amount of any losses that the entity would have to assume as a result.

D. The potential liquidity support from the parent company, shareholders or, in general, related parties, at the local or international level, the opportunity and term of this support and the costs to be assumed.

E. Possible liquidity support from the Central Bank, its requirements, costs, opportunity and term.

F. Communication plans to the supervisor, stakeholders, the public and the media, in case of rumours or dissemination of information that may negatively affect the entity's liquidity.

G. Prioritization processes that detail when and how each action can and should be executed, with a high degree of flexibility that allows the Entity to respond quickly and in an informed manner in different situations.

H. Specification of roles and responsibilities, the authority to invoke the liquidity contingency plan, the officials and areas in charge of its implementation, as well as the constitution of the crisis group (composed of different areas of the entity) that facilitates internal coordination and communication for decision-making during a period of liquidity crisis.

I. Evaluation and testing process on operation, where the strategic and operational aspects of the plan are tested, including the protocols to follow, the communications strategy, the operability of the available liquidity lines and the roles and responsibilities that each of the officials involved must perform.

4. COUNTRY RISK MANAGEMENT

4.1. Definition of country risk

This refers to the possibility that the Entity may incur losses from financial transactions abroad due to a deterioration in the economic and/or sociopolitical conditions of the recipient country, whether due to restrictions on foreign exchange transfers or factors beyond the recipient country's control regarding its commercial and financial status. This definition includes, among others, Sovereign Risk (SR) and Transfer Risk (TR), which are associated with such factors.

Sovereign risk (SR): It is the probability that the Entity will incur losses in its financial operations abroad, caused by the non-compliance of financial obligations in charge of a State or of obligations guaranteed by it.

Transfer Risk (TR): This is the probability that the Entity will incur losses due to non-compliance by a debtor or economic agent domiciled abroad, because of the inability to have foreign currency to service the debt, remit the profits or the value of the investment.

For the purposes of this section, a financial operation is understood to be the capital investments made by the supervised Entities abroad directly and indirectly.

4.2. Components

4.2.1. Stages

4.2.1.1. ID

The Entity will at all times identify the country risk to which it is exposed, based on the business plan, risk appetite, type and characteristics of the financial operations carried out, the economic and socio-political conditions of the country receiving the operation, problems of foreign exchange transfers or factors not attributable to the commercial and financial condition of the country receiving the operation, and which would result in the partial or total loss of its value.

4.2.1.2. Measurement

The Entity will quantify the level of exposure to country risk inherent in its financial operations abroad, assessing its likelihood of occurrence and its severity should it materialize.

Therefore, the Entity will design and implement a prospective methodology for assessing country risk and establish the criteria to be considered in determining whether there is a detriment to financial operations abroad. This methodology, at a minimum, begins with an analysis of the economic, social, and political situation of each country where its financial operations are domiciled and also considers that country's present and future capacity to conduct international transactions, to meet the obligations arising from them, and to have the necessary information to identify events that could affect its ability to fulfil its financial commitments.

In assessing country risk, the Entity will conduct at least two types of analysis: (i) a baseline analysis, based on financial, economic, and market indicators, and (ii) a supplementary analysis, which focuses on political, institutional, and social aspects, as well as other relevant information that allows the Entity to evaluate the country risk exposure of its financial operations abroad. These analyses will be performed periodically and must allow the Entity to effectively monitor economic, social, and political changes occurring in the jurisdictions where it makes its capital investments.

4.2.1.2.1. Baseline analysis

The Entity will evaluate quantitative factors that include the following elements:

A. Economic indicators

An analysis must be conducted to allow the Entity to assess the country's economic situation, incorporating the trends of the following indicators: Gross Domestic Product (GDP) and aggregate demand indicators (consumption and investment), inflation, unemployment, fiscal balance (deficit, debt trajectory, and composition of domestic and external debt), interest rates, and the external sector, primarily evaluating the exchange rate, the current account balance, and the capital account balance,

including, in this case, the variation in international reserves. The series of variables used in this analysis must cover a period of 10 years.

B. Market indicators

An analysis should be conducted to assess market confidence, investor risk perception, the availability and cost of external borrowing, and countries' sovereign capacity to meet their external financial obligations and access international credit markets. To this end, sovereign risk ratings from at least two internationally recognized rating agencies should be considered, and the analysis should incorporate, when available, the evolution of indicators such as Credit Default Swaps (CDS) and the sovereign debt spread (EMBI).

The Entity will evaluate the performance of the leading indicators of the sector in which the Entity made the investment abroad.

C. Supplementary analysis

This includes all aspects not covered in the baseline analysis, but which are crucial for a complete country risk assessment. To this end, the Entity must analyse the following factors:

a. Political, institutional, and social

An analysis should be carried out of information related to the political, legal and institutional stability of the country, and particular social conditions of each nation that may generate deterioration in the willingness or capacity to fulfil its obligations abroad.

Similarly, consideration must be given to the existence or possibility of occurrence of political, corruption, social or war conflicts internal or with other countries, which may endanger the economic stability of the country or directly or indirectly affect the financial operations of the Entity carried out in it.

An analysis of compliance with regulations established in the financial system of the country receiving the investment with respect to international prudential standards may also be included.

b. Natural hazards

The analysis of the risk to which investments abroad are exposed due to the possible occurrence of natural phenomena such as earthquakes, hurricanes, floods, among others, which may affect the countries receiving the Entity's operations and consequently impact the value of the investment, must be considered.

c. Other factors

The analysis should consider factors that impact the credit relationships of the recipient countries of the financial operation with private or multilateral banks, as well as any restrictions that may exist on international financial transactions.

Additionally, the analysis must include other indicators that the Entity considers appropriate according to the conditions of each country, and which must be incorporated to carry out an adequate and comprehensive risk assessment.

4.2.1.2.2. Stress tests

The Entity must conduct stress tests at least annually to assess its resilience to risk factors that exacerbate its exposure to country risk. However, in the event of persistent and severe occurrences that significantly deteriorate the economic and/or political conditions of the country receiving the investment, the Entity must increase the frequency of these tests.

Stress tests should consider scenarios in which adverse movements in the economic, market, social and/or political indicators used to perform the basic and complementary analysis referred to in sections 6.3.1.2.1 and 6.3.1.2.2 of Part II of Chapter XXXI of the CBCF may affect the value of the operation abroad and consequently deteriorate the financial strength of the entity.

The Board of Directors must promptly be informed, monitor and, if necessary, comment on the results of the stress tests and incorporate them into its decision-making process to design actions aimed at preventing losses in the value of the Entity's investments in the face of adverse scenarios exacerbated by this risk.

4.2.1.3. Control

The Entity must take the necessary measures to mitigate the occurrence of country risk to which its financial operations abroad are exposed, which must be incorporated within the entity's risk control and management structure.

This stage must meet the following minimum requirements:

A. Maintain proportion with the volume and complexity of the financial operations carried out by the Entity abroad, so that there is a correspondence between the model, risk appetite and the type of operations carried out.

B. Consider the entity's business plan, the mechanisms and procedures for carrying out financial operations, as well as the economic, social, and political conditions of the country where they are located.

C. To allow for the monitoring of country risk exposure levels and the limits established by the entity, as well as to adopt measures to counteract country risk exposure, including the stress tests referred to in section 6.3.1.3 of this Part.

D. Define the mechanisms, procedures and administrative bodies responsible for compliance with country risk limits.

4.2.1.4. Monitoring

The guidelines and procedures established for implementing this stage will allow the Entity to monitor its exposure to country risk. Therefore, this stage must, at a minimum:

A. Maintain correspondence with the volume, business plan, risk appetite and complexity of the financial operations carried out by the Entity abroad.

B. To continuously monitor economic, social and/or political or other events that may negatively impact the Entity's investment abroad.

C. To carry out continuous monitoring of the levels of exposure to country risk and of the general and special limits established by the entity, according to its structure, characteristics, authorized operations and considering the risk appetite of the entity.

D. Prepare management and country risk monitoring reports, at least semi-annually, that allow the Entity to properly monitor and make decisions to mitigate the level of exposure to this risk.

4.2.1.4.1. Boundaries

For the proper management of country risk, the Entity will establish limits consistent with its business plan, risk appetite, financial strength, and systemic importance, as well as with the economies and markets in which it operates. These limits must allow the Entity to control exposures that exceed its risk tolerance levels. In this regard, it must define, at a minimum:

A. Exposure limits by country, geographic area, foreign currency type, among others.

   Parameters from which jurisdictions eligible to be the destination of financial operations abroad are defined, according to the size, appetite and tolerance for risk, the business plan and the systemic importance of the entity.

In defining these limits, the Entity will consider the performance of operations with the participation of related parties, including intragroup operations, which, because they are domiciled in the same country receiving the financial operation, imply exposure to country risk.

4.2.2. Reports

The person(s) performing the risk management function will submit a report to the Board of Directors and the Legal Representative, at least semi-annually, containing at least the following aspects:

A. The entity's exposure and overall concentration level to country risk, broken down by country, geographic area, foreign currency type, and other factors. This also includes the entity's intragroup and related-party exposures at the regional and country levels.

B. General compliance with the policies and limits on country risk exposure authorized by the JD.

C. The results of the evaluation and monitoring of the behaviour of the variables used in the measurement stage referred to in subparagraph 6.3.1.2 of Part II of Chapter XXXI of the CBCF, as well as the country risk ratings and the adjustment for impairment of the investment in accordance with the provisions of paragraph 6 of Part III of Chapter XXXI of the CBCF.

This report will be submitted to the SFC at intervals no greater than six months.

5. CONDUCT RISK MANAGEMENT

5.1. Definition of Conduct Risk

Conduct risk refers to the possibility of loss, sanction, or reputational damage arising from actions, decisions, or omissions by the company, its directors, or employees that deviate from standards of good practice, create conflicts of interest, undermine market confidence, or harm clients or end investors.

Likewise, the Financial Superintendence defines conduct risk as:

"It consists of the possibility of affecting the rights of the financial consumer or the market, arising from a practice of a Supervised Entity (hereinafter, "Supervised Entity")."

The definition of Conduct is understood as follows:
"Behaviors and practices carried out by Supervised Entities that materially impact or may cause harm to financial consumers or to the integrity and transparency of the markets."

5.2 Scope and Application

For the Company, the scope of conduct risk is assessed in relation to:

- Direct client (Ashmore Investments UK Limited and Larrain Vial S.A. Comisionista de Bolsa)
    - As defined by the Royal Spanish Academy:
        - Investor: *"A natural or legal person who makes an investment of funds."*
        - Qualified: *"Possessing specialized training to perform a professional activity or a specific job."*

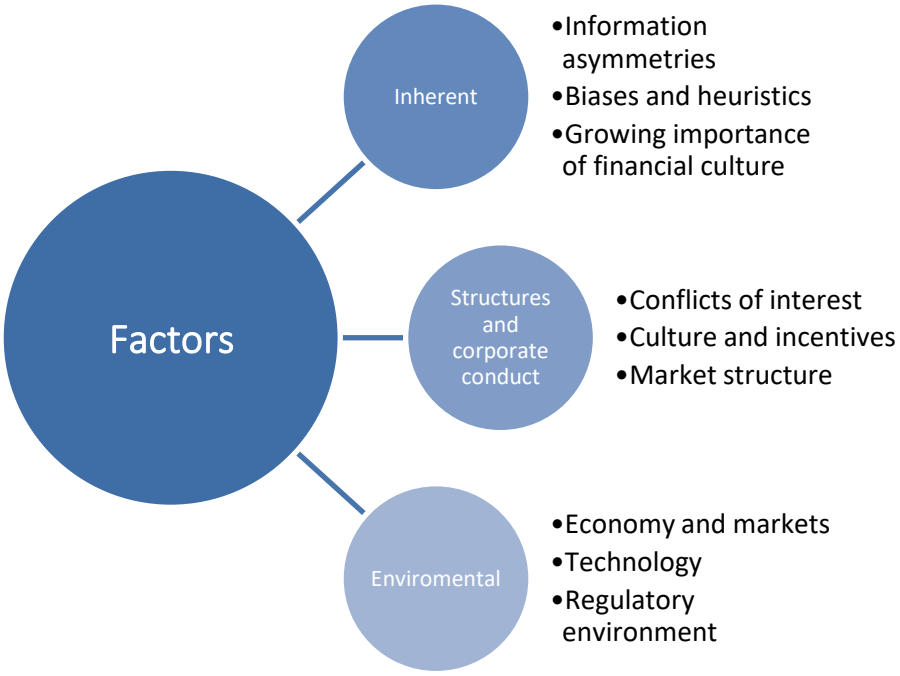
5.2.

- Company employees
- Company senior management

5.3 Guiding Principles

- Primacy of the client's and/or ultimate beneficiary's interest.
- Transparency and traceability in decision-making.
- Prevention of insider trading.
- Active management of conflicts of interest.
- Zero tolerance for improper or perverse incentives.
- Fair calibration of fees and costs for the managed vehicle.
- Strong governance: "Conduct before profitability."
- Responsibility regarding public trust in fiduciary activity.
- Principle of Fair Treatment, ensuring access to clear, transparent, and timely information, aligned with the financial consumer's needs and profile.

5.4 Key Factors of Conduct Risk



When defining the role of business processes within conduct risk management, the following points should be considered:

- **Inherent:**
  - Information asymmetries: Not applicable to the Company's operations, as no party has privileged access to relevant information. Qualified investors have the technical capacity and sufficient experience to understand the risks and characteristics of the products offered.
  - Biases and heuristics: This factor typically refers to consumers making poorly informed decisions or being influenced by inadequate recommendations. In the case of qualified investors, their level of expertise allows them to make informed and strategic

decisions, minimizing such biases.
    - Growing importance of financial culture: The presumption of financial knowledge is valid in this context, given that the Company's clients have extensive market experience and do not require additional financial education to understand fiduciary products or services.
- **Structures and corporate conduct:**
    - Conflicts of interest: The Company has two main clients, one domiciled in Colombia and the other in the United Kingdom. The likelihood of conflicts of interest is low; however, the Company has a formal policy for managing these risks. Furthermore, this point is more relevant to retail markets, which does not apply due to the wholesale nature of the operation.
    - Culture and incentives: The Company maintains a robust compliance program, including ongoing training in corporate best practices and professional ethics, aligned with the standards of its parent group.
    - Market structure: The Company operates under a solid, documented market structure that supports the efficient management of its fiduciary operations.
- **Environmental:**
    - Economy and markets: The Company continuously adapts to economic and financial conditions, adjusting its strategies to meet the specific needs of its qualified clients.
    - Technology: The Company adopts technology and cybersecurity policies defined by its parent company, ensuring international standards for information protection and digital operations.
    - Regulatory environment: The Company performs monthly regulatory updates, enabling it to anticipate and adapt to regulatory changes impacting the structure of financial market

5.5 Relevant Sources of Conduct Risk for the Company

Within operations involving qualified investors, the following sources of conduct risk are identified, understood as situations that may negatively impact fiduciary relationships, institutional reputation, or regulatory compliance:

Source	Specific Risk	Application to the Model
Financial advisory	Biases in recommendations or undue preferences	Possible favoring of group interests in investment decisions, despite client expertise.
Vehicle management	Prioritization of institutional interests over client's	Risk in asset selection or execution timing that does not reflect the best option for the investor.
Insider information	Improper use or leakage of information in cross-border operations	Reputational and legal risk due to mishandling of sensitive information.
Internal governance	Lack of independence in strategic decisions vis-à-vis parent company	Risk of strategic or operational subordination compromising autonomy in key decisions.
Relationship with	Ambiguity in roles and	Risk in allocation of

administrator	responsibilities as intermediary client	responsibilities.

5.6 Controls and Mitigation Measures

- Technical reference document on conduct risk, aligned with regulatory standards and best practices.
- Annual training for operational and management teams, emphasizing ethical management, conflicts of interest, and fiduciary standards.
- Document traceability in recommendation and investment decision-making processes.
- Periodic integrity and compliance declarations by the team.
- Internal and external channels for reporting irregularities (Whistleblowing Policy).
- Continuous oversight by the Company's Committees.

5.7 Monitoring and Reporting

- Annual training on ethical culture and conduct standards.
- Periodic reporting to the Audit Committee and Board of Directors.
- Annual review of conduct risk, in line with guidelines from the Financial Superintendence of Colombia.
- Inclusion of early warnings in the Risk Matrix, monitored by the compliance area.

5.8 Responsibilities

Governing Bodies	Role
Board of Directors	Risk appetite and oversight
Compliance Officer	Implementation and management
Risk Director	Monitoring and testing
Internal Audit	Independent review

6. CREDIT RISK MANAGEMENT

6.1. Definition of credit risk

For the purposes of the trust company, credit risk is the possibility that the entity may incur losses or that the value of its assets may deteriorate because of the total or partial non-compliance with the obligations assumed by a debtor or counterparty.

Within the framework of this Chapter, the term "debtor" shall be understood to include not only the principal obligor, but also co-debtors, guarantors, joint debtors and, in general, any natural or legal person who directly or indirectly is or may become obligated to pay an obligation.

References to credit agreements, active credit operations, credit assets, loan portfolios or operations also include financing agreements, leasing, factoring, guarantees granted, firm financing commitments, contingent limits and any other operation that generates or may generate exposure to credit risk.

6.2. Scope and Application of the SARC

AIAC Trustee, in the exercise of managing its own resources, autonomous assets and investment

funds, is exposed to credit risk, understood as the possibility of losses arising from the non-compliance with contractual obligations by issuers of securities (Issuer Risk) or counterparties in financial operations (Counterparty Risk).

Aware of this exposure, the Entity has a Credit Risk Management System (CRMS) that allows it to effectively identify, measure, manage, and control the risks associated with managed portfolios, Collective Investment Funds, and its Proprietary Position. This system is developed in accordance with the Trust's risk appetite profile and framework, its business plan, the nature, size, complexity, and diversity of its operations, as well as its relevance due to its size and interconnectedness within the financial system and the economic and market environments in which it operates.

This document defines the general guidelines of the SARC, including policies, procedures, measurement methodologies, internal control mechanisms and responsibilities of the management, administration and control bodies, to ensure timely and effective decisions for risk mitigation.

The Risk Department is responsible for preparing this document, and its approval rests with the Board of Directors, the highest decision-making body regarding policies, procedures, and methodologies related to credit risk management. The Risk Committee, as an advisory body, evaluates and analyses all aspects of risk management, issuing opinions, recommendations, and alerts to the Board of Directors. The document is updated periodically to reflect changes in the credit risk management and control system and is shared with all relevant departments for their awareness and implementation.

6.3. Exceptions

Within the scope of application of the Comprehensive Risk Management System (SIAR), AIAC Trustee will not be obliged to adopt the instructions indicated in this section when it falls under any of the following scenarios:

a. When it carries out activities or manages legal businesses that, by their nature, fall under special risk management regimes, typical of other entities such as: exchange intermediation and financial services companies, general deposit warehouses, livestock funds, pension and severance fund management companies, social security funds and entities managing the solidarity regime of average premium with defined benefit, as well as insurance and reinsurance intermediaries.

b. Regarding the resources from savings accounts and/or accounts whose abandoned balances are transferred as a loan in favour of the Special Fund administered by ICETEX, in accordance with the provisions of Law 1777 of 2016, Decree 2555 of 2010 and other applicable regulations.

c. In those cases where, by legal or regulatory provision, special risk management regimes are applied that are exclusive of these instructions, such as Specialized Companies in Electronic Deposits and Payments (SEDPE), International Financial Institutions (INFI) and other entities with a special regime for risk management.

6.4. Credit Risk Management System

The Entity has methodologies appropriate to the complexity and level of credit risks involved in its activities that allow it to measure and quantify the expected losses derived from exposure to credit risk. The Credit Risk Management System methodology consists of four elements, namely: Identification, Measurement, Control and Monitoring.

6.4.1. ID

The Financial Risk Management Department identifies the various credit risks to which the Company's portfolio and the portfolios of third parties it manages are exposed, in accordance with current regulations, actual market conditions, and the definition of authorized operations. For the Company, the authorized operations and investment policy are defined in the Investment Policy and Limits document; for Collective Investment Funds, in the respective Regulations; and for Fiduciary businesses, in the Contract.
This stage is completed from the incorporation of new products and throughout the life of the portfolios.

6.4.2. Measurement

The credit risk assessment process is performed for all positions held by the Business Units in treasury operations, unless the investor or settlor of a specific Business Unit expressly indicates their wish to exempt AIAC Trustee from performing such assessment. Furthermore, a business client may request a different assessment than AIAC Trustee's standard assessment, in which case the risk department must validate the assessment before incorporating it into the contract.
The primary internal metric in the credit risk measurement process is the Issuer and Counterparty Quota Model. Ultimately, this yields the overall credit risk of the portfolio's holdings, considering the degree of offsetting both between the holdings themselves and between the different types of risk.
The internal risk methodology implemented by the Entity and its corresponding updates incorporate at least quantitative criteria that allow the identification of the value at risk.
In the case of the own position, it will be applied according to the model and quotas stated by the parent company and by the Corporate Risk Unit.

The risk area performs the analysis based on the possible sources determined according to the type of entity and its geographical location; thus, according to the possibility of information, these possibilities exist:

- **Local Issuer:** In the case of an issuer in the Colombian market, the most recent risk rating issued by a recognized rating agency under the supervision of the Financial Superintendency of Colombia is identified. Additionally, the Trust Company's Credit Unit is asked to provide its non-binding opinion on the entity, and a financial analysis is performed using the CAMEL model. Furthermore, the analysis is supported by any additional information available, giving priority to the most recent data.

- **International Issuer:** If the issuer is not part of the Colombian market, the analysis begins with the latest international risk ratings issued by globally recognized rating agencies. The most common rating among those available is then identified, considering the rating equivalency tables established by Bloomberg. The model, and as a matter of policy, uses the lowest rating when there are differing rating levels among recognized market rating agencies.

Having all possible sources of financial and general information about the entity and the issuer under study, the rating process is carried out by weighting the information, resulting in an internal rating of the potential issuer and/or counterparty.

The sources and the internal rating are evaluated and compared with the Fiduciary Framework, which serves as a reference guide for the maximum percentages permitted per issuer according to the level of risk, financial analysis, and qualitative assessment. The process described determines the feasibility of allocating a credit line to the requested Issuer or Counterparty, as well as the amount, if approved.

6.4.2.1. Rating Agencies and Risk Assessment Methodologies

The investment policies of Collective Investment Funds and Managed Assets define the minimum acceptable ratings for issuers. Local and international rating agencies assign short-term (≤1 year) and long-term (>1 year) ratings according to the risk of the issuer or counterparty.

6.4.2.2. Local Rating Agencies:

Fitch Ratings Colombia: Qualitative assessment supported by quantitative analysis. Scales: short term from F1+ to E, long term from AAA to E.

BRC Investor Services: Evaluates payment capacity, asset quality, funding, operational stability, and risk management. Scales: short-term from BRC 1+ to BRC 6, long-term from AAA to E.

Value and Risk: Scales like the previous ones, used as an additional reference for credit risk.

6.4.2.3. International Rating Agencies:

Fitch Ratings International: Rating based on internal methodologies, issuer information and reliable independent sources.

Moody's: Applies JDA methodology, considering financial strength and external support. Scales: long term from AAA to C, short term from P-1 to NP.

Standard & Poor's: Approach based on general principles, complemented by sector and region-specific methodologies.

6.4.2.4. CAMEL Methodology:

Adopted to evaluate entities in the Colombian financial sector using indicators of Capital, Asset Quality, Management, Profitability, and Liquidity. The data is obtained from financial statements reported to the Financial Superintendency.

- Profitability: operational efficiency and return on assets.
- Asset Quality: portfolio and its coverage.
- Stability: ability to absorb losses.
- Liquidity: liability structure and availability of funds.
- Administration: efficiency of administrative expenses versus operational expenses.

6.4.2.5. Internal Qualification Unification Model:

It integrates and weights ratings from different sources to obtain a single risk rating of the issuer or counterparty, adjusting the weight of the information according to its availability and relevance.

6.4.3. Control

AIAC Trust has credit risk control mechanisms that allow it to monitor compliance with investment policies and the respective risk levels that have been defined for the different portfolios managed.
Control activities include monitoring maximum credit risk exposure limits, alert levels, the general investment policy defined in regulations or contracts, those of a regulatory nature, and those corresponding to monitoring internal limits.
Monitoring is performed daily or at the minimum frequency established by current regulations. The results are reported in the Financial Risk Management's daily and monthly reports, including reports of overages and excesses, as well as the most relevant variations in credit risk metrics. These reports serve as the primary risk input for portfolio management by the investment area.
The limits for Proprietary Position are defined by AIAC's Corporate area, reviewed annually or more frequently if required, and reported to the Trust's Financial Risk Management for compliance. The Investment Policy is reviewed at least annually and is communicated to and submitted to AIAC Trust's Financial Risk Management for monitoring.

6.4.4. Monitoring

The monitoring phase aims to assess the reasonableness of the risk measurements implemented in the credit risk management models, along with the corresponding follow-up of issuers and counterparties. AIAC Trust, considering the exposure in its managed portfolios, reviews the methodologies and limits established by the Financial Risk Management department on an annual basis.
Thus, the Risk Management department periodically monitors relevant quantitative and qualitative information from entities, different sectors, outlooks and reports from rating agencies, among others… to identify early warnings and make the necessary adjustments, allowing the adoption of measures to avoid impacts on managed resources and portfolios.

Therefore, the following monitoring mechanisms have been established:

- Credit risk measurement models.
- Counterparty and issuer risk models (CAMEL).
- Control and monitoring of concentration indicators by issuer, counterparty, credit exposure of derivatives, as well as daily alerts with daily monitoring.
- Daily monitoring of operations with counterparties.

7. CREDIT EXPOSURE ACCEPTANCE AND MONITORING CYCLE

Within the framework of managing investment portfolios and independent assets, AIAC Trustee will manage the credit risk derived from its exposures to issuers and counterparties, following a process equivalent to the credit cycle, adapted to its role as administrator:

7.1. Admission of counterparties and issuers:
- Define eligibility criteria, risk tolerance levels and concentration limits by issuer, sector, instrument type and credit rating.
- Base the selection on analysis of payment capacity, solvency, contractual conditions and macroeconomic environment.

7.2. Prior information and transparency:
- Have sufficient and up-to-date information on the issuer or counterparty, including risk rating, financial conditions and associated guarantees (if applicable).

7.3. Assessment of ability to pay:
- Analyse financial indicators, cash flows, debt level, compliance history and risks associated with the business or project financed by the issuer.

7.4. Evaluation and assessment of guarantees:
- When guarantees exist, verify their suitability, coverage and ease of realization, in accordance with applicable technical and legal criteria.

7.5. Monitoring and control:
- Perform periodic monitoring of credit exposures, reclassify when necessary and assess impacts of changes in financial, macroeconomic or market conditions.

7.6. Managing deterioration situations:
- Define procedures for the negotiation, restructuring or divestment of at-risk positions, with the objective of minimizing losses and maximizing recoveries.

This process will be adjusted to the institutional risk appetite and current regulatory provisions, ensuring that decisions are made based on technical analysis and prudential criteria.

8. EXPOSURE LIMITS AND MONITORING:

AIAC Trustee manages its Collective Investment Funds and Proprietary Position within the established regulatory limits, complementing them with internal limits and alerts defined in the investment regulations, specifically regarding issuer and counterparty quotas, in accordance with the methodology approved by the Board of Directors.
In the case of the Proprietary Position, the investment limits respond to the allocations defined by the corporate areas and include specific restrictions for deposits in savings and current accounts, approved according to the internal policies of the Trustee.

The definition of limits includes, at a minimum:

- Exposure thresholds by portfolio, term, economic sector and counterparty, in accordance with the provisions of Decree 2555 of 2010.
- Allocation quotas and their approval processes.

These limits are established considering the results of stress tests for credit risk and are complemented by intensified monitoring procedures when they approach internal or regulatory limits, along with timely corrective measures.

Monitoring is conducted daily to ensure that investments in each fund or portfolio do not exceed approved limits or the guidelines defined in prospectuses or investment frameworks, which establish maximum levels for asset groups with similar characteristics. The Financial Risk Area reports any alerts and excesses detected daily to Investments and General Management.

For publicly traded third-party portfolios, internal alerts are governed by current regulations. For non-public portfolios, the Credit Risk Model and the Issuer Risk Model, both approved by the Board of Directors, are applied.

The Risk Management Department is responsible for monitoring and reporting compliance with limits, either daily or as established by regulations or the Board of Directors. The Investment Area and portfolio managers must immediately correct any deviations that may affect the objectives and risk profile of each portfolio, in accordance with the procedure defined by the Trust Company.

9. ROLES AND RESPONSIBILITIES IN THE SARC

The Entity's organizational structure is suitable for comprehensive risk management, with clearly assigned functions and responsibilities for each level:

9.1. Board of Directors (BOD)

The highest governing body for risk matters. Its functions include approving and overseeing the business plan, the Risk Appetite Framework (RAF), the policies and limits of the Risk and Compensation System (RCS), the risk governance structure, and the strategies for managing risk, capital, liquidity, and conflicts of interest. It evaluates the effectiveness of the RCS, approves corrective actions, reviews the results of stress tests, defines the training policy, and appoints the Risk Committee and its regulations.

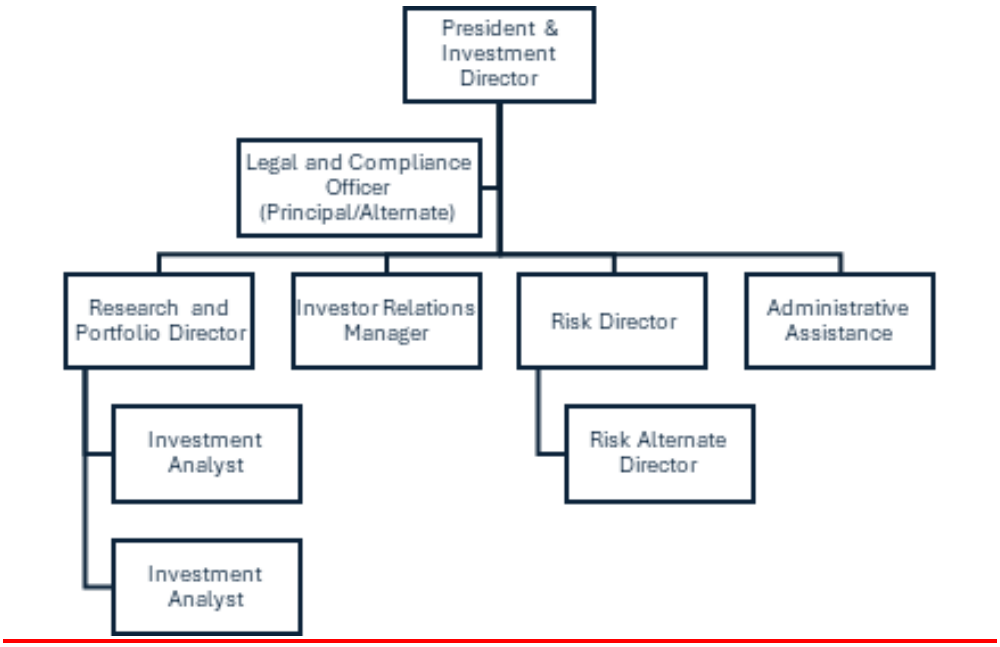
9.2. Legal Representative (RL)

Responsible for executing and overseeing the implementation of the Risk and Compensation System (RCS) and the business plan according to Board guidelines. Submits policies, limits, and strategies for approval; approves the RCS document, contingency and continuity plans; ensures their inclusion in the budget; monitors the system's adequacy and the diversification of assets and liabilities; guarantees the quality and consistency of information; and periodically reports to the Board and the Superintendency of Finance (SFC) on risk management, relevant changes, or events that affect the viability of the business.

9.3. Financial Risk Unit

Independent area with authority and direct access to the Board of Directors, Risk Committee, and Senior Management. Leads the design, updating, and monitoring of the Risk Management Framework (MAR) and the Risk Assessment and Risk Management System (SARC) document; develops policies, methodologies, limits, controls, and indicators; evaluates business continuity plans; monitors risk exposure, limit compliance, and exceptional operations; conducts stress tests and reports results. Manages the operational risk event log and issues daily, weekly, monthly, and quarterly reports to the relevant bodies on risk levels, deviations, market conditions, and emerging risks, proposing corrective measures and improvement actions.

The AIAC Trust Company's risk unit will be structured as follows:



9.4. Risk Committee

A body composed of an odd number of members, chaired by someone independent of the Board of Directors and with experience in risk management. It meets at least quarterly. Its main functions are:

- Monitor the risk profile and appetite, its consistency with the business plan, capital and liquidity, and report to the Board of Directors with recommendations.
- Advise on operations, events or new markets that may affect risk exposure, generate deviations or compromise the viability of the business.
- Review SARC policies annually and propose adjustments.
- Advise on risk culture and evaluate the business continuity plan.
- Analyse the monthly reports from the risk unit and communicate conclusions to the Board of Directors.

9.5. Control Bodies

They include at least Statutory Auditing and Internal Auditing.

9.6. Statutory Audit:

Periodically evaluate compliance with risk management and include an annual report in the financial statement audit, available to regulatory bodies. Promptly inform the shareholders' meeting, board of directors, legal representative, and the Superintendency of Finance (SFC) of any significant irregularities or deficiencies, documenting findings, suggested actions, and the entity's responses. In the case of FIC (Financial Investment Corporation), an external auditor may be contracted according to regulations, without replacing the statutory audit.

9.7. Internal Audit:

An independent body that reports to the Board of Directors and Management Committee. It evaluates the effectiveness of the Risk and Compliance System (RCS), including related-party transactions and flows, and reports the results to the risk management, liability, audit committee, and Board of Directors areas. It monitors recommendations and action plans derived from internal and SFC assessments and reports to the SFC on material situations and corrective actions not required.

10. TECHNOLOGICAL INFRASTRUCTURE AND INFORMATION SYSTEMS

AIAC Trustee has the technological infrastructure, data architecture, and information systems necessary for comprehensive credit risk management, regulatory compliance, and timely decision-making. This infrastructure supports both internal operations and the handling of requests from regulatory bodies and other stakeholders, through policies and procedures that define communication channels, reporting methods, and frequency.
The systems allow:

- Collect, update and maintain complete and truthful information on the payment status of issuers, counterparties and debtors, immediately reflecting any changes.
- Maintain records and databases that support risk management models, including financial, sociodemographic, guarantee, compliance history and relevant correspondence information.
- Have security mechanisms in place to ensure the confidentiality, integrity, quality, availability, and consistency of information, with access restricted to authorized personnel.
- Ensure the preservation of the minimum information for 7 years, as established by current regulations.
- Adopt procedures for the timely attention and rectification of information, as well as for the immediate submission of updated data to risk centres.

Main technological tools:

Controls and responsibilities:

- An official appointed by the Principal Legal Representative oversees the operation and updating of the applications, ensuring the immediate registration of changes and their submission to credit bureaus.
- Risk Management and portfolio managers use these tools to continuously monitor risks and take necessary actions.

11. CONTINUITY AND CONTINGENCY PLANS:

The organization has documented plans within its Information Security system, including policies, procedures, response times, and responsible departments, to ensure business continuity in the event of unplanned incidents. Testing is conducted regularly with the participation of all departments involved in critical business processes.

12. SUPERVISION BY THE SFC

Within the scope of its legal powers and pursuant to Article 325 of the EOSF, the Financial Superintendency of Colombia (SFC) supervises and evaluates AIAC Trustee's credit risk management policies and practices, as well as the proper implementation of approved or unobjected models. Based on this evaluation, the SFC may adopt any measures it deems necessary, including non-objection, rejection, or replacement of the model, as well as other administrative actions provided for in current regulations.

The SFC considers any significant failure in credit risk management that could compromise the solvency or liquidity of the entity to be an unsafe practice. This includes, among others:

- Reversing provisions or improving ratings of issuers or counterparties without complying with approved methodologies or without full verification of established minimum criteria.
- Carrying out restructurings or modifications of conditions without a duly documented financial viability analysis.

In the event of finding serious deficiencies, the SFC may order:

- The immediate suspension of the use of internal models that have not been challenged, applying the SFC reference model on a temporary basis until the observations are corrected.
- The initiation of a recovery program in accordance with Decree 2555 of 2010, in addition to any applicable institutional or personal sanctions.

AIAC Trustee guarantees that all credit risk management practices strictly comply with regulatory provisions and approved methodologies, maintaining traceability and documentary support to back up the decisions made.

12. AGGREGATION OF RISK DATA AND REPORTING

12.1 Definition of risk data aggregation

Define, collect and process data on all risks to which the Entity is exposed to present reports that allow it to evaluate its performance based on its risk appetite framework.

12.2 Principles

A. Governance: Consolidating risk data and risk reporting practices should be based on sound guidelines provided by the legal representative and the Board of Directors.

B. Accuracy and integrity: Generate accurate and reliable data on risks, which should be aggregated, primarily, in an automated way.

C. Completeness: Identify and aggregate all data on significant risks within the entity. This data must be available at a minimum by risk, activity, asset type, economic sector, region, and intragroup transactions and transactions with related parties.

PART III. STANDARD RISK MEASUREMENT AND REPORTING

1. INTRODUCTION

To achieve adequate measurement and/or reporting of market, operational, liquidity and country risks, under homogeneous standards, as well as to allocate impairment (hereinafter provisions), liquidity and capital necessary to cover market and operational risk, the entity established the following methodologies.

2. MARKET RISK MODEL

2.1. Measurement methodology - Standard measurement model

The Entity must:

A. Implement the standard model (see **Annex A** of the MAR) for measuring market risk arising from treasury book positions and spot transactions. Additionally, implement the standard model for measuring market risk for those investment funds and other funds they manage, in accordance with the instructions set forth in Annex 7 of Chapter XXXI of the CBCF.

B. Report the results of the market risk measurement in the formats established in Annex 7 of Chapter XXXI of the CBCF.

2.2. Accounting Disclosure

Entity d will present a summary of its treasury operations in the notes to the financial statements. These notes will contain qualitative and quantitative information about the nature of the operations and illustrate how these activities contribute to its revenue and market risk profile.

2.2.1. Qualitative Information

Qualitative information reports on advanced risk management practices, indicating compliance with policies, limits, and the level of exposure to market risk. This information will include business objectives, strategies, and risk-taking philosophy, as well as a description of the various inherent risks arising from the business itself, categorized by type and source.

Qualitative information is essential for preparing and providing a better understanding of the Entity's financial statements. Likewise, the Entity should use qualitative information to illustrate how treasury operations align with the organization's business objectives.

The Entity shall disclose whether its market participation can generally be considered that of a market maker, or whether it corresponds to proprietary trading. Finally, the information disclosed must consider potential changes in risk levels, material changes in trading strategies, exposure limits, and risk management systems.

2.2.2. Quantitative Information

AIAC will provide the public with a clear picture of its treasury activities by presenting quantitative information. This presentation will include the following information:

A. Composition of treasury portfolios.

B. Maximum, minimum and average values of treasury portfolios during the analysis period.

C. Risk exposure levels for the most important financial instruments within treasury portfolios.

D. Risk exposure levels for the consolidated treasury position.

2.3. Reports to the SFC

The results of the market risk assessment will be reported to the SFC with the frequency and according to the requirements established in the formats provided for this purpose. Additionally, the SFC may request any supplementary information it deems necessary.

3. MODEL FOR MEASURING AND RECORDING OPERATIONAL RISK EVENTS

3.1. Measurement model

The Entity uses the methodology for determining the weighting factor for calculating the value of the exposure for operational risk, as well as the registration of operational risk events proposed by the Financial Superintendency of Colombia (See Annex B of the MAR).

3.2. High-quality operational risk event log

The proper identification, collection, and processing of records of the Company's operational losses are essential requirements for the proper management of operational risk. For operational risk management, the entity must maintain a high-quality operational risk event log that includes the general and specific criteria referred to in subsections 4.2.2.1 and 4.2.2.2 of Part III of Chapter XXXI of the CBFC, which must be kept permanently updated and available to the SFC. This log must contain all operational risk events that have occurred that:

A. They generate losses and affect the entity's income statement.

B. They do not generate losses and therefore do not affect the entity's income statement.

These events must be disclosed in accordance with the terms of this Part.

It is important to note that, for the cases in subparagraph b) of this section, the measurement will be qualitative and quantitative when so determined by the entity.

3.2.1. General criteria for recording operational risk events

For the collection of internal data and construction of the database with historical records of operational risk events, entities must take the following into account:

A. Entities must have documented procedures and processes for the identification, collection and treatment of operational risk event records.

B. Records of operational loss events must be comprehensive and include all activities and exposures, as well as encompass all operational risk events.

C. Each entity must maintain its own unique operational risk event log. Entities with an international parent company must have information related to local operational risk events available and centralized in Colombia.

D. The level of detail in the descriptive and quantitative information must correspond at least to the following fields:

Name	Description
Reference	Internal code that relates the event sequentially.
Event start date	Date the event begins. Day, month, year, hour.
Event end date	Date the event ends. Day, month, year, hour.
Date of discovery	Date the event is discovered. Day, month, year, hour.
Accounting registration date	Date on which the loss from the event is recorded in the accounts. Day, month, year, hour.
Recovery date	Date on which the money used to address an operational risk event is fully or partially recovered. Day, month, year, hour.
Badge	Foreign currency in which the event takes place.
Gross amount	The amount of money (legal currency) that represents the gross loss. The record must include the items listed in subparagraph 4.2.2.2.1 of this Part.
Total amount recovered	The amount of money recovered through direct action by the entity. Includes amounts recovered through insurance.
Amount recovered by insurance	This corresponds to the amount of money recovered through insurance coverage.
Number of other recoveries	This refers to the amount of money recovered through mechanisms other than insurance coverage.
Net number of recoveries	The amount of money (legal currency) that the loss amounts to, considering the total amount recovered.

Name	Description
Operational risk class	Specify the risk class, according to the classification adopted in subparagraph 4.2.2.2.4 of this Part.
Affected product/service	Identify the affected product or service.
Affected Accounts	Identify the affected CUIF accounts.
Process	Identify the affected process.
Type of loss	Identify the type of loss, in accordance with the classification adopted in subparagraph 4.2.2, paragraphs a) and b) of this Part.
Event description	Detailed description of the event.
	- Customer service or support channel (when applicable)
	- Geographical area
Business lines	Identification according to the classification adopted by the SFC in sub-item 4.2.2.2.3 of this Part.

E. For the construction of the operational risk event record, entities may use additional fields to those described above.

F. All activities of supervised entities must be allocated among the business lines specified in subparagraph 4.2.2.2.3 of this Part, ensuring that each activity corresponds to only one business line and that no activity remains unassigned. To this end, the entity must have systematic information and procedures for allocating net financial income, which entails the allocation of both financial income and expenses.

G. Entities must document and keep available to the SFC the criteria they will consider classifying the different activities in each of the lines of business, without prejudice to complying with the following principles:

   a. Any operational risk event that occurs during an activity related to a main activity must be classified under the line of business that corresponds to the main activity.

   b. When a loss event affects more than one line of business and one of the lines generates 50% or more of the total losses, the total value of those losses should be allocated to that operating line.

   c. When a loss event affects more than one line of business and none of the lines involved generates 50% or more of the total losses, the corresponding value should be assigned to each affected line of business.

   d. When an operational risk event occurs for a line of business, it must be recorded according to its classification in the first, second and third level of disaggregation detailed in the table of sub-item 4.2.2.2.4 of this Part.

H. Entities must have an operational control process designed to independently review the integrity and accuracy of operational risk events.

3.3. Accounting disclosure

Without prejudice to other accounting disclosure requirements, when losses caused by the occurrence of an operational risk event affect the income statement, they must be recorded in expense accounts in the period in which the loss materialized.

Recoveries for operational risk, when they affect the income statement, must be recorded in income accounts in the period in which the recovery is made effective.

The required expense and income accounts will be defined by this Superintendency in the respective CUIF.

3.4. Reports to the SFC

The SFC may request any information it deems relevant in relation to operational risk management.

4. LIQUIDITY RISK MODEL

4.1. Measurement methodology

The Entity developed an internal model for liquidity risk measurement that meets the minimum requirements established by the Financial Superintendency of Colombia, as described in the MAR.

4.2. Accounting disclosure

The Entity will present in the notes to the financial statements a summary of its liquidity risk position. In this regard, the notes will contain qualitative and quantitative information on the nature and amount of expected cash flow mismatches for the timeframes between one day and one month, as specified in Chapter XXXI of the CBCF for liquidity risk management, and will illustrate how the Entity's various activities contribute to its liquidity risk profile.

Without prejudice to the functions assigned in other provisions, the statutory auditor shall verify at least once every six months the strict compliance with the provisions of Chapter XXXI of the CBCF regarding liquidity risk management and include an express and detailed statement on such management within the opinion on the financial statements. Likewise, pursuant to Article 207, paragraph 3, of the Commercial Code, the statutory auditor must promptly inform the legal representative and the SFC of any material irregularities observed in compliance with the liquidity risk instructions of Chapter XXXI of the CBCF.

4.3. Reports to the SFC

The results of the liquidity risk measurement will be reported to the SFC with the established periodicity in the formats provided for this purpose.

5. COUNTRY RISK MODEL

AIAC developed a prospective methodology for measuring country risk that meets the minimum requirements established by the Financial Superintendency of Colombia, as described in the MAR.

5.1. Country risk disclosure

Without prejudice to other applicable provisions on financial disclosure, the Entity shall present in the notes to the financial statements of the period in question, qualitative and quantitative information on performance and financial position, management strategies and practices, exposures and impairment due to country risk, at a global level, by geographic region and by each country, in order to facilitate the effective understanding of the entity's risk exposures during a financial reporting period.

The Entity has an analysis of the country's categorization in accordance with the provisions of external circular 018 and the MAR.

PART IV. DEFINITIONS

The following definitions should be considered for the purposes of this document:

A. Activity: It is a product, line, branch, business unit, subordinate entity or process that the entity develops to carry out its business plan.

B. Significant activity: It is a product, line, branch, business unit, subordinate entity or process that is fundamental for the entity to carry out its business plan and to achieve its main objectives.

C. Senior management (SM): This is the group of people responsible for risk management and who report directly to the Board of Directors and/or the legal representative, including the latter.

D. The Managing Director, under the direction and supervision of the Board of Directors, is responsible for directing, executing, and monitoring the entity's operations, consistent with the business plan, risk appetite, and other policies.

E. Risk appetite: The level(s) and types of risk that the entity is willing to assume to meet its

business plan.

F. Back office: This area is responsible for the operational aspects of treasury functions, specifically the closing, recording, and final authorization of transactions. In other words, it is responsible for processing, ensuring the fulfilment of transactions, and their valuation.

G. Risk capacity: The maximum level of risk that an entity can assume given its current level of resources before failing to comply with legal controls, liquidity limits, and/or compromising business continuity.

H. Financial consumer: This refers to any client, user, or potential client of the supervised entities, as defined in Article 2 of Law 1328 of 2009.

I. Risk culture: It is a set of attitudes, values, norms, guidelines and sanctions for responsible behaviour from which the members of an entity understand, assume, manage and discuss the inherent risks of the activities carried out by the entity and are responsible for acting and making decisions within the framework of risk appetite and the limits established for the assumption of risks.

J. Entity: That entity supervised by the SFC to which the provision in which the term is used applies, except for the financial holdings referred to in Law 1870 of 2017. Additionally, when referring to an entity, it is understood that it refers to both individually and as a consolidated entity.

K. Risk governance structure: It is a structure that allows the Board of Directors and the General Manager to establish and make decisions on the strategy and approach to risk, articulate and monitor the adherence of risk to the business plan, and identify, measure, control and monitor risks.

L. Comprehensive risk assessment: A comprehensive and joint assessment of risks, including the relationships between them, without prejudice to the differences inherent in each type of risk and its management.

M. Event: A fact or change that may affect the achievement of the entity's objectives.

N. Operational risk event: This is any event or change that may generate losses for the entity due to operational risk.

O. Risk factors: Risk factors are understood to be the sources that generate risks, which may or may not result in losses. Risk factors include human resources, processes, technology, infrastructure, and external events. These factors should be classified as internal or external.

P. Front office: This is the area responsible for securities trading, closing and registering

transactions in trading systems, customer relations and/or the commercial aspects of the treasury.

Q. Bank book: The bank book is made up of all positions arising from: (i) the operation of attracting funds by entities through current and savings accounts, term deposits, the issuance of bonds, etc.; (ii) the loan portfolio; (iii) the establishment of guarantees and sureties; (iv) investments to maturity, and in general; (v) any operation that is not part of the treasury book.

R. Treasury book: The treasury book comprises all positions resulting from treasury operations that the entity maintains to benefit in the short term from asset price fluctuations, as well as from investments sensitive to market fluctuations. Accordingly, the treasury book includes, among other things, all marketable investments available for sale.

S. Middle office: Risk management unit.

T. Treasury operations: These are foreign exchange market operations, fixed income, variable income and those securities indexed to a reference rate or index, except for own issues; money market operations; operations with derivatives and structured products; and in general, any other that is carried out in the name of the entity or for its benefit or on behalf of third parties.

U. Related parties: These are natural or legal persons who have with all or some of the entities that make up the financial conglomerate, or with the individual supervised entity in case it is not part of a financial conglomerate, management, direct and indirect ownership links equal to or greater than 5% and companies where any of the persons mentioned above have a direct or indirect participation equal to or greater than 10%.

V. For the purposes of calculating indirect participation, the instructions given in sub-item 2.3.2.1 of Chapter XIII-16 of the CBCF must be considered.

W. References to related parties in this Chapter shall be understood to apply to liquidity risk management.

X. Risk profile: Exposure to current and potential risks inherent in the development of the entity's business plan.

Y. For the purposes of section 4 of Part II and Part III related to operational risk management, the risk profile is understood as the consolidated result of the ongoing measurement of the risks to which the entity is exposed.

Z. Contingency plan: A set of actions and resources to respond to adverse situations, failures, and specific interruptions of a system or process, as well as to address vulnerabilities identified in stress tests. The plan must be realistic, feasible, and consistent with the business plan and risk appetite.

AA. Business Continuity Plan (BCP): It is the detailed set of actions, procedures, systems and resources necessary to respond, recover, resume and restore the operation of the entity in case of internal or external interruptions that affect its normal functioning.

BB. Contingency funding plan: It is the compilation of policies, procedures and action plans to respond to severe shocks that affect an entity's ability to fund some or all its activities on time and at a reasonable cost.

CC. Business plan: It is the detailed plan of the objectives to be achieved, in the development of its activities, specifying how it will be achieved, the necessary activities to implement and in what times they will be executed, considering the mission, vision and objectives of the entity.

DD. Stress tests: These are simulations of adverse events and scenarios to assess the impact of each risk on exposure. Entities may follow the guidelines in Chapter XXVIII of the CBCF regarding internal stress tests (used for financial planning and risk management), as well as the information and modelling developed for the tests required by the SFC (for prudential supervision and financial stability assessment).

EE. Rediscount operations: A rediscount operation is understood to be one in which a financial institution authorized by law to carry out these operations channels resources for the promotion of economic activities in specific sectors through entities authorized for this purpose and subject to the supervision of the SFC, except for insurance intermediaries.

FF. Inherent risk: This is the probability that an entity will incur a loss because of its exposure to present and future events, before applying mitigation mechanisms. This includes current and potential risks.

GG. Net risk: This is the result of mitigating inherent risks through operational management and the risk governance structure.

HH. Early warning system: A system that allows for the early identification of possible deviations in risk appetite, limits, and/or increases in exposure levels.

II. Treasury: Areas that deal with customer relations and commercial aspects, negotiation or trading, identification, measurement and control of market risk, compliance and recording of treasury operations.

JJ. Risk tolerance: This is the acceptable level of variation or deviation from the risk appetite that the entity is willing to accept in the development of its business plan. It is measured in absolute or percentage terms.

KK. New Products Committee (CNP): body responsible for approving new products and assets for

the Trust.

LL. Conflict of interest: a situation in which a person, due to their activity, faces different alternatives of conduct in relation to incompatible interests, none of which they can privilege in view of their legal or contractual obligations.

MM. First-Line Controls: controls generated during process management, by risk owners, and by those responsible for risk management. These functions are directly aligned with the delivery of the product or service.

NN. Second-line controls: controls associated with supervisory and compliance functions. In terms of credit risk, the responsible area at AIAC is the Financial Risk Management department.

OO. Credit Risk (CR): This is the possibility that a counterparty will default on its payment obligations related to a specific transaction. This risk is frequently referred to by different names depending on its source or the surrounding circumstances. Thus, the credit risk of trading transactions, and especially that of derivatives (off-balance sheet transactions), is often called counterparty risk, since in this case the exposure does not always cover the full nominal amounts of the transaction, but only the loss that would be incurred by having to replenish the trades in the market.

PP. Liquidity Risk (LR): This is the possibility that an entity may incur losses due to the contingency of not being able to fully meet, in a timely and efficient manner, expected and unexpected, current and future cash flows, without affecting the course of daily operations or the entity's financial condition. Liquidity risk can be represented by funding liquidity risk and market liquidity risk.

QQ. Funding Liquidity Risk: is the insufficiency of available liquid assets to meet the cash flows of an entity or the need to assume unusual funding costs.

RR. Market Liquidity Risk: This occurs when the Entity's ability to generate or unwind financial positions at market price is limited, either because there is not enough market depth or because there are drastic changes in rates and prices.

SS. Market Risk (MR): is the possibility that an entity may incur losses associated with the decrease in the value of its portfolios or the portfolios of third parties that are under its management due to variations in the price of the investments in which it maintains positions within or outside the balance sheet.

TT. Strategic Risk: This is the risk that an institution faces due to strategic decisions, the business environment, and competition. It is divided into (i) strategic positioning risk, when the institution is not being managed in accordance with its strategy, and (ii) strategy execution risk, when the strategy is not being executed correctly.

UU. ESG risk: risks that impact the business associated with environmental factors (climate change and carbon emissions, use of natural resources and water management, pollution and waste management, eco-design and innovation), social factors (health, safety, diversity and workforce training, responsibility to customers and product, community relations and charitable activities) and governance factors (shareholder rights, composition of the Board of Directors, Management Compensation Policy, Fraud and bribery).

VV. Legal Risk (LRG): is the possibility of loss incurred by an Entity when it is sanctioned or obliged to compensate for damages because of non-compliance with rules or regulations and contractual obligations.

WW. Operational Risk (OR): This is the possibility that the entity may incur losses due to deficiencies, failures, or inadequate functioning of processes, technology, infrastructure, or human resources, as well as due to the occurrence of external events associated with these. It includes Legal Risk.

XX. Benchmark portfolio: a reference portfolio used to measure the performance of a managed investment portfolio.

YY. Third-party managed portfolios: Includes independent trusts and pension portfolios.

ZZ. Business Unit: AIAC Trustee's organizational structure whose purpose is to manage or administer the resources of a trust, an independent estate, or an investment fund