

Principal Grupo Financiero  
México,  
Principal Fondos de  
Inversión, S.A. de C.V.,  
Operadora de Fondos de  
Inversión, Principal Grupo  
Financiero

SOC 1<sup>®</sup> – System and Organization Controls  
for Service Organizations: Internal Control  
over Financial Reporting

January 1<sup>st</sup> – December 31<sup>st</sup>, 2023

*With Management's Assertion and Independent  
Service Auditor's Report, including Tests  
Performed and Related Results*



## Table of Contents

<b>Section I – Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos de Inversión Investors’ Investment Management Processing Services Assertion .....</b>	<b>4</b>
<b>Section II – Independent Service Auditor’s Report.....</b>	<b>6</b>
<b>Scope .....</b>	<b>6</b>
<b>Scope Limitations.....</b>	<b>6</b>
<b>Operadora de Fondos de Inversión responsibility .....</b>	<b>7</b>
<b>Service auditor’s responsibilities .....</b>	<b>7</b>
<b>Inherent limitations .....</b>	<b>8</b>
<b>Description of tests of controls.....</b>	<b>8</b>
<b>Opinion .....</b>	<b>9</b>
<b>Restricted use .....</b>	<b>9</b>
<b>Section III – Operadora de Fondos de Inversión Investment Management Processing Services.....</b>	<b>10</b>
<b>Scope .....</b>	<b>10</b>
<b>Overview of the Organization .....</b>	<b>10</b>
<b>Information and Communication.....</b>	<b>17</b>
<b>Monitoring Activities .....</b>	<b>17</b>
<b>Description of the Processing Environment .....</b>	<b>17</b>
<b>Investment Management Systems.....</b>	<b>18</b>
<b>Investment Management Processing Services .....</b>	<b>18</b>
<b>New Account and Account Maintenance .....</b>	<b>18</b>
<b>New Security Setup and Maintenance .....</b>	<b>19</b>
<b>Trade Processing.....</b>	<b>20</b>
<b>Securities Trading.....</b>	<b>20</b>
<b>Trade Allocation .....</b>	<b>21</b>
<b>Best Execution Review.....</b>	<b>21</b>
<b>Trade Settlement Procedures.....</b>	<b>22</b>
<b>Valuation.....</b>	<b>22</b>
<b>Investment Income &amp; Corporate Actions.....</b>	<b>22</b>

Reconciliations .....	<b>23</b>
Client Reporting .....	<b>23</b>
Privacy Program .....	24
Business Continuity Program .....	25
Information Security Program .....	28
Record Retention Policy .....	31
Information Technology Controls .....	332
System Development, Maintenance, Documentation and Change/Release Control .	<b>332</b>
Physical Access Restrictions.....	<b>34</b>
Logical Access Administration.....	<b>36</b>
Computer Operations.....	<b>37</b>
Complementary User Entity Controls (CUECs).....	37
Section IV – Description of Control Objectives, Controls, Tests and Results of Testing .....	388
Overview of Internal Controls.....	388
Section V – Other Information Provided by Operadora de Fondos de Inversión.....	62



## **Section I – Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos de Inversión Investors’ Investment Management Processing Services Assertion**

We have prepared the description of Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos de Inversión y Principal Grupo Financiero (Hereafter “Operadora de Fondos de Inversión”) Investment Management Processing Services system entitled, Section III – Operadora de Fondos de Inversión Investment Management Processing Services (Hereafter “Description”) for processing user entities’ transactions throughout the period January 1<sup>st</sup>, 2023 to December 31<sup>st</sup>, 2023 and their auditors who audit and report on such user entities’ financial statements or internal control over financial reporting and have a sufficient understanding about controls implemented and the system, when assessing the risks of material misstatements of user entities’ financial statements. The Description includes only the control objectives and related controls of Operadora de Fondos de Inversión and excludes the control objectives and related controls of the subservice organizations.

We confirm, to the best of our knowledge and best practices, that:

- a) The Description fairly presents the system of the Investment Management Process (System) made available to user entities during the period January 1<sup>st</sup>, 2023 to December 31<sup>st</sup>, 2023 for processing their transactions as it relates to controls that are likely relevant to user entities’ internal control over financial reporting. The criteria we used in making this assertion are included as follows:
  1. Presents how the Description made available to user entities of the system was designed and implemented to process relevant transactions, including, if applicable:
    - The types of services provided.
    - The procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the System.
    - The information used in the performance of the procedures including, if applicable, information involved in initiating, authorizing, recording, processing, and reporting transactions and the manner the System captures and addresses significant events and conditions, other than transactions.
    - The process used to prepare reports and other information for user entities.

- The specified control objectives and controls designed to achieve those objectives.
  - Other aspects of our control environment, risk assessment process, information, and communication systems (including the related business processes), control activities, and monitoring activities that are relevant to the services provided, including processing and reporting transactions of user entities.
2. Includes relevant details of changes to the System during the period covered by the Description.
  3. Does not omit or distort information relevant to the System, while acknowledging that the Description is prepared to meet the common needs of a broad range of user entities of the System and their user auditors and may not, therefore, include every aspect of the System that each individual user entity of the System and its user auditor may consider important in the user entity's own particular environment.
  4. The risks that threaten the achievement of the control objectives stated in the Description have been identified by management of Operadora de Fondos de Inversión.
  5. The controls identified in the Description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the Description from being achieved; and
  6. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

## Section II – Independent Service Auditor’s Report

The Board of Directors  
Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos de Inversión y Principal  
Grupo Financiero  
Operadora de Fondos de Inversión

### Scope

We have examined Operadora de Fondos de Inversión description entitled Section III – Operadora de Fondos de Inversión (Description) throughout the period January 1<sup>st</sup>, 2023 to December 31<sup>st</sup>, 2023 of its Investment Management Process (System) for processing user entities’ transactions and the suitability of the design and operating effectiveness of controls described therein to achieve the related control objectives stated in the Description based on the criteria identified in Section I – Operadora de Fondos de Inversión Investment Management Processing Services Management Assertion (Assertion). The Control Objectives and controls included in the Description are those that management of Operadora de Fondos de Inversión believe are relevant to user entities’ internal control over financial reporting and the Description does not include those aspects of the System that are not likely to be relevant to user entities’ internal control over financial reporting.

The Description indicates that certain Control Objectives can be achieved only if Operadora de Fondos de Inversión controls are suitably designed and operate effectively, along with related controls at the service organization.

Operadora de Fondos de Inversión uses BlackRock to provide the Aladdin application platform used in the generation and management of information on the Afore (retirement funds) and Investment Funds as a trading platform, and SIIF to manage the portfolio of funds and Soluciones to manage accounting.

The Description includes only the Control Objectives and related controls of Operadora de Fondos de Inversión and including general controls of Aladdin, SIIF and Soluciones as systems used for the operation. The Description also indicates that certain Control Objectives specified by Operadora de Fondos de Inversión can be achieved only if controls are suitably designed and operate effectively.

The information included in *Section V – Other Information Provided by Operadora de Fondos de Inversión* is presented by management to provide additional information and is not part of the Description.

Information about the Privacy Program, Business Continuity, Incident Response, Disaster Recovery Program, Information Security Program and Data Retention and Destruction has not been subject to the procedures applied in our examination of the description of the System and of the suitability of the design and operating effectiveness of controls. We express no opinion on it.

## **Scope Limitations**

The following activities were reviewed with an understanding of the processes, but not as an evaluation of controls:

1. Privacy Program
2. Business Continuity Program
3. Disaster recovery program
4. Information security program
5. Records Retention Policy

## **Operadora de Fondos de Inversión responsibility**

Operadora de Fondos de Inversión has provided the assessment about the fairness of the presentation of the Description and suitability of the design and operating effectiveness of the control. Operadora de Fondos de Inversión is responsible for providing and confirming the Description and assessment including the completeness, accuracy and method of presentation of the Description and specifying the Control Objectives and stating them, also, identifying the risks that threaten the achievement of the Control Objectives, selecting the criteria stated in the assessment and designing, implementing and documenting controls that are suitably designed and operating effectively to achieve the related Control Objectives.

## **Service auditor's responsibilities**

Our responsibility is to express an opinion on the fairness of the presentation of the Description and the suitability of the design and operating effectiveness of the controls described to achieve the related Control Objectives. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Based on our examination, we obtain reasonable assurance about whether, in all material respects, based on the criteria in management's Assertion, the Description is fairly presented, and the controls were suitably designed and operated effectively to achieve the related Control Objectives throughout the period January 1<sup>st</sup>, 2023, to December 31<sup>st</sup>, 2023. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

1. Performing procedures to obtain evidence about the fairness of the presentation of the Description and the suitability of the design and operating effectiveness of the controls to achieve the related Control Objectives.
2. Assessing the risks that the Description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related Control Objectives.
3. Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related Control Objectives were achieved.
4. Evaluating the overall presentation of the Description, the suitability of the Control Objectives, and the suitability of the criteria specified by the service organization in the Assertion.

## **Inherent limitations**

The Description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the System that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related Control Objectives, is subject to the risk that controls at a service organization may become ineffective.

Additionally, due to the nature of the automatic controls, walk-through testing and evaluation of the controls was performed during 2024.

## **Description of tests of controls**

The specific controls tested, and the nature, timing and results of those tests are listed in the accompanying *Section IV – Description of Control Objectives, Controls, Tests and Results of Testing* (Description of Tests and Results).



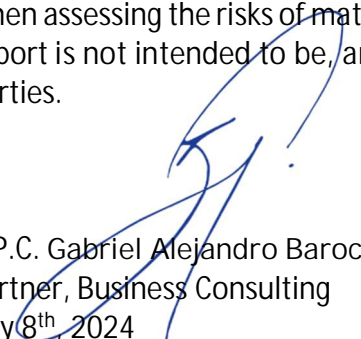
## Opinion

In our opinion, in all material respects, based on the criteria described in Operadora de Fondos de Inversión Assertion:

- a) The Description fairly presents the System that was designed and implemented throughout the period January 1<sup>st</sup>, 2023 to December 31<sup>st</sup>, 2023.
- b) The controls related to the Control Objectives were suitably designed to provide reasonable assurance that the Control Objectives would be achieved if the controls operated effectively throughout the period January 1<sup>st</sup>, 2023 to December 31<sup>st</sup>, 2023.
- c) The controls operated effectively to provide reasonable assurance that the control objectives were achieved during the period from January 1, 2023 to December 31, 2023, given that complementary controls were taken from the subservice organization and of the user entity in the design of BlackRock controls, for the general controls of the Aladdin application; effectively operated during the entire period from January 1, 2023 to December 31, 2023.

## Restricted use

This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of management of Operadora de Fondos de Inversión, user entities of Operadora de Fondos de Inversión System during the period January 1<sup>st</sup>, 2023 to December 31<sup>st</sup>, 2023 and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.



C.P.C. Gabriel Alejandro Baroccio Pompa  
Partner, Business Consulting  
July 8<sup>th</sup>, 2024

Mancera, S.C. EY Mexico, Mexico City  
Part member of Ernst & Young Global Limited

## **Section III – Operadora de Fondos de Inversión Investment Management Processing Services**

### **Scope**

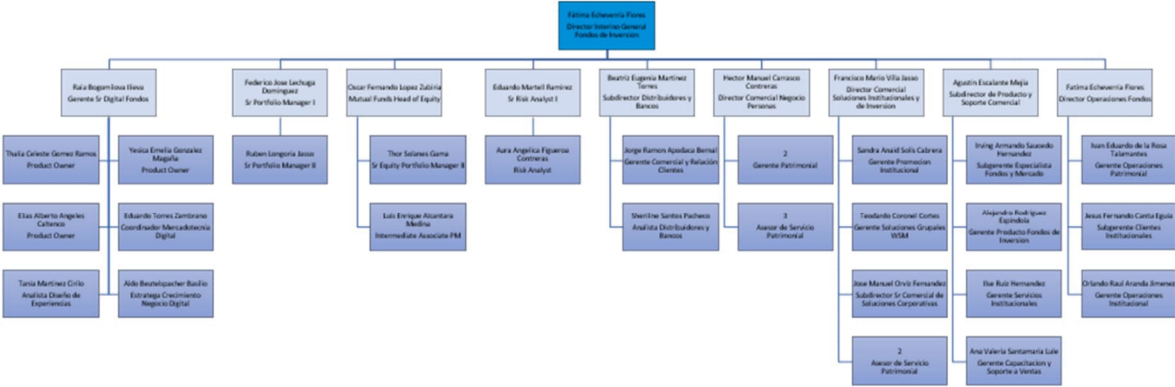
This report covers the investment management operations for institutional clients of Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos de Inversión y Principal Grupo Financiero of the period January 1st, 2023 to December 31st, 2023. It does not include other operations of affiliates.

### **Overview of the Organization**

Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos de Inversión is an indirect wholly owned affiliate of the Principal Financial Group, which operates in Mexico mainly through three business: *Principal Afore* (retirement funds), *Principal Fondos de Inversión*, *Operadora de Fondos de Inversión* (Investment Funds) and *Principal Compañía de Seguros* (life insurance) helping people and companies to plan and build their financial wellbeing. Founded in 1993, Operadora de Fondos de Inversión is one of the most active, fastest growing and expanding companies with 16% of participation in the financial Mexican market.

Operadora de Fondos de Inversión works with approximately 2.7M of clients in Mexico managing assets approximately MXN \$193 billion, operating a wide range of investments on behalf of institutional, central banks, pension clients, mutual funds, and other commingled products for distribution to individual investors and smaller institutional clients. It is to be noted, Principal Financial Group has operations in the NASDAQ stock exchange, however, Operadora de Fondos de Inversión does not have operations in any stock exchange market.

# Organizational chart of Operadora de Fondos de Inversión



## Governance Structure

Based on the legal scheme applicable to Principal Grupo Financiero Mexico, Operadora de Fondos de Inversión has a robust Corporate Governance Structure which is responsible for monitoring and supervising the management conducted over the investment funds. This structure is conformed as follows:

- a) Shareholders; with ordinary, extraordinary, and special meetings held at least once a year and which results decisions must be followed as long as these comply with internal and external regulations.
- b) Commissioner; responsible for issuing an annual report of the reasonableness of the financial information presented by the Board of Directors and the compliance of internal and external regulations.
- c) Board of Directors: integrated by at least five members and no more than fifteen, including responsibilities, but not limited to:
  - General Power of Attorney for Acts of Administration.
  - Subscribe, accept, issue, endorse and guarantee all kinds of credit instruments on behalf of the Company.
  - Open and cancel bank and investment accounts and/or securities on behalf of the Company.
  - Appoint or remove the CEO, external auditor, Management and other officers, proxies, agents, and employees of the Company.

- Approve the Financial Statements of the Company.
- d) Investments Committee: integrated by four members from the Risk Management, Investments and Regulatory Controllershship Departments, with meetings held on a monthly basis to determine the investment strategy over the traded securities in compliance with the statements of the Mexican authority Comisión Nacional Bancaria y de Valores (CNBV).
- e) Communication and Control Committee: responsible of the prevention and detection of acts, omissions or operations that could promote assistance or cooperation, of any kind, for the commission of the crime related to terrorism or operations with resources of illegal origin.
- f) Risk Committee: responsible for identifying, assessing and managing the risk that could impact the operation of the Company.
- g) Financial Products Analysis Committee (CRAPF): responsible for establishing and implementing the policies, procedures and guidelines indicated in the *Circular de Servicios de Inversión*.
- h) Fiduciary Committee: including responsibilities, but not limited to:
- Discuss and approve new fiduciary business.
  - Discuss and approve policies for customer adoption, hiring, management and control of all those operations derived from fiduciary services.
  - Being notified of the resolutions in relation to the periodical evaluation results of clients experience.
- i) Chief Executive Officer (CEO): responsible for implementing business plan, the guidelines of the Board of Directors, the design of the organizational structure, the internal control system, the observance of regulations as well as lead the development of the Company operations.
- j) Regulatory Controller: responsible for supervising and monitoring the integrity, prestige and quality of the services provided by the Company in compliance with the internal and external regulations.
- k) Risk Management Responsible: define policies, procedures, controls, and guidelines for risk management; supporting actions to identify, measure, monitor, limit, control, report and disclose in a timely and systematic manner to the Board of Directors and the Risk Committee about the exposure to quantifiable and non-quantifiable risks.

- l) Chief Compliance Officer (CCO): including responsibilities, but not limited to:
  - Elaborate the Compliance Manual.
  - Notify any conduct, activity or behavior carried out by the directors, officers, employees, or attorneys, which cause an infringement over the Law or the Compliance Manual, in order to impose the disciplinary measures, accordingly.
- m) Responsible for Supervising the compliance with Investment Services.
- n) Compliance Supervisor of Investment Services in the Advised Investment Services modality: responsible for verifying compliance related to the evaluation applied to the clients profiles and the reasonable analysis of financial products.
- o) External Audit.
- p) Internal Audit.

### **Operadora de Fondos de Inversión External Party Interactions**

On a daily basis, Operadora de Fondos de Inversión interact with various external parties in connection with providing services for clients. A brief description of the nature of these external parties' interaction with Operadora de Fondos de Inversión includes:

1. Clients: individuals involved with the oversight, management, or administration of investors. Clients communicate their investment guidelines and objectives to Operadora de Fondos de Inversión and they are provided with periodic performance reports.
2. Custodians/Financial Administrators: financial institutions that hold the assets and may serve as the book of record (valuation agent) on behalf of clients. Custodians and Financial Administrators are hired by the client. The custodian is responsible for the receipt, delivery and safeguarding of client assets. Custodians provide periodic reports to Operadora de Fondos de Inversión.
3. Counterparties: referring to government, national banks, national monetary authorities, and international monetary organizations that act as the ultimate guarantor for loans and indemnities. Also, counterparty can refer to brokers, investment banks, and other securities dealers that serve as the contracting party when completing "over the counter" securities transactions.

4. Pricing and Other Information Vendors: responsible for providing daily and monthly securities' prices and corporate action notifications for application to clients' portfolios. Examples of pricing and other information vendors include Proveedor Integral de Precios (PiP), Thomson Reuters, Standard and Poor's (S&P) and Bloomberg. Operadora de Fondos de Inversión utilizes PiP as the primary pricing service, working closely to help to ensure accurate security pricing is received. Operadora de Fondos de Inversión can communicate with PiP in the event that pricing of a security does not seem to reflect market activity by providing trade information.
5. Research Vendors: Operadora de Fondos de Inversión utilizes a number of different sources of investment research, including broker and third-party services. While some research might be sources from outside the Company, the analysts and Portfolio Managers are ultimately responsible for the formulation of the strategies and execution thereon.
6. Information Technology and Application Consulting Services: vendors that provide software as a service and back-end support on the applications used by the Company.
7. Legal: external firms on legal matters involved with investment management and private placement activities.

## **Compliance and Quality**

Operadora de Fondos de Inversión has three quality schemes to support the compliance approach over its operations. First, the main operative areas looking for the enhancement of the daily operations; secondly, the Regulatory Controllershship that provide guidelines over the compliance of internal and external regulations; and the Process Improvement Department that helps to enhance the clients and employees experience. In addition, Operadora de Fondos de Inversión has the ACA Compliance Group certification to verify that Operadora de Fondos de Inversión complies with the Global Investment Performance Standards (GIPS).

## **Overview of Internal Control**

A company's internal control is a process – effected by an entity's Board of Directors, management, and other personnel – designed to provide reasonable assurance regarding the achievement of objectives related to the:

- Reliability of internal and external financial and non-financial reporting;
- Effectiveness and efficiency of the entity's operations, and;
- Adherence to laws and regulations to which the entity is subject.

The following is a description of the five components of internal control as defined in the Internal Control – Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission in 2013 for which Operadora de Fondos de Inversión is utilizing.

## **Control Environment**

The control environment is the set of standards, processes, and structures that provides the basis for carrying out internal control across the organization. It is the foundation for all other components of internal control, providing discipline and structure. The control environment of Operadora de Fondos de Inversión is the responsibility of the Chief Executive Officer (CEO) who establishes the tone at the top regarding the importance of internal control, including expected standards of conduct.

Management of Operadora de Fondos de Inversión recognizes its responsibility for establishing, communicating, and monitoring control policies and procedures. Importance is placed on maintaining sound internal control and the integrity and ethical values of all personnel. The resulting control environment has a pervasive impact on the overall system of internal control.

Integrity and Ethical Values: The Principal Global Code of Conduct (the Code) serves as the foundation for ethical behavior across the organization and provides an uniform set of principles for how Board members and employees are accountable for adhering to the Code, conducting business, and performing their duties. The Code is internally communicated through the intranet and is also publicly available on the Company website. Moreover, Principal Grupo Financiero Mexico has an Ethics and Compliance Program, which promotes the core value of Integrity and it is applicable to the entire organization. Key aspects of the program include:

- High level commitment;
- Ethics and Compliance Risk Assessment;
- Documented policies, standards and procedures;
- Training and communication on ethics and compliance;
- Due diligence;
- Hotline;
- Program Monitoring and oversight;
- Discipline and incentives, and;
- Response and improvement of the Program.

The CCO is responsible for monitoring the compliance of the Ethics and Compliance Program along with the Regulatory Controllershship and Compliance Officers across Principal Grupo Financiero Mexico. Directors and employees are expected to promptly report suspected violations of the Code or laws and suspected unethical or fraudulent activities.

Additionally, there are established policies and procedures covering investment management operations. These policies are high-level statements that set strategic direction, expectations and scope for various topics and are mandatory for those employees in the stated scope of the policy. The standards define what the organization will do to achieve related policies.

## **Risk Assessment**

An entity's risk assessment process involves a dynamic and iterative process for identifying, analyzing, and managing risks to the achievement of its objectives, including assessing risks relevant to the preparation of its financial statements and to clients.

Risk Identification and Assessment: Corporate Risk Department of Principal Grupo Financiero Mexico (PGFM) is responsible for the identification, assessment and management over the risk that may impact in the operations or the financial information of the Company. Likewise, there are Risks Departments at a business unit level (*Principal Afore*, *Principal Fondos de Inversión Operadora de Fondos de Inversión* and *Principal Compañía de Seguros*) that monitor the risks related to the investment management.

At a corporate level, the risk management model is defined under three lines of defense: the first one is formed by the operative areas; they own the risks that they identify, evaluate, control and mitigate; their processes are executed in adherence to internal policies and procedures, as well as the applicable internal and external regulations, always consistent with the goals and objectives of the Company. The second line, is responsible for defining policies and procedures that allow a proper management and control of the risks, providing guidelines to the operative areas in order to comply with the abovementioned. Finally, the third line is the Corporate Internal Audit Department to provide independent assurance over the risk management and internal control performed by the first and second lines of defense.

The Corporate Risk Department is independent from the operative areas, thus avoiding conflicts of interest and ensuring an adequate segregation of duties. It also performs frequent monitoring of operational processes to supervise the process control environment.

## **Control Activities**

Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of objectives. Control activities, whether preventive or detective, automated or manual, have various objectives and are applied at various organizational and functional levels.

The Internal Controls Over Financial Reporting Policy and supporting Standards provide that all areas of Principal maintain certain internal control policies and procedures to help ensure



transactions are properly authorized and accounted for in an accurate and timely manner. They also require that assets be properly safeguarded, adequate segregation of duties and control responsibilities are established and maintained in all functional areas of Principal, and each area has effective ongoing monitoring procedures that ensure transactions, processes and activities are functioning effectively. Specific control activities are provided in the Control Environment, Investment Management Processing Services, and Information Technology Controls portions of *Section III*, as well as listed in *Section IV – Description of Control Objectives, Controls, Tests and Results of Testing*.

## **Information and Communication**

Information and communication processes support the identification, capture, and exchange of relevant information from both internal and external sources in a form and timeframe that enable people to carry out their responsibilities. PGFM has established corporate policies and standards to address information requirements, including identifying data attributes, information repositories, and retention. Information systems consist of procedures, whether automated or manual, to initiate, authorize, record, process, and report transactions and maintain accountability for the related assets, liabilities, and equities.

Communication is the continual, iterative process of obtaining, sharing, and providing necessary information both internally and externally as appropriate. It includes ensuring individual roles and responsibilities and related information pertaining to internal controls are clearly understood. Communication systems exist from an entity-level to a department-level. Multiple communication paths exist to help ensure that processes function as designed and issues are identified and resolved in a timely manner. Internal and external reporting and control processes provide sufficient communication of relevant information and necessary analysis time.

## **Monitoring Activities**

Monitoring is a critical aspect of internal control in evaluating whether processes and controls at different levels of the entity are operating as intended and whether they are modified as appropriate for changes in conditions. As the first line of defense, operative areas are responsible for the ongoing operation of effective controls and management personnel are responsible for monitoring the quality of internal control performance as a routine part of their activities. In addition, various second line functions provide ongoing monitoring of Investment Management risks and controls on a regular basis, working closely with line management.

## **Description of the Processing Environment**

Servers are hosted at two geographically distant data centers interconnected with owned high-speed optic fiber. The production data center is located Apodaca, Nuevo León and the

disaster recovery data center located in San Pedro Garza García, also in Nuevo León, Mexico. Security over these distributed systems is provided by the native security features of the Microsoft Windows operating system, coupled with application- level security.

## **Investment Management Systems**

The Investment Management Systems are composed of the following applications used to record and monitor the investments underlying the client and separate accounts managed by Operadora de Fondos de Inversión:

- Aladdin is a purchased third-party investment application provided by BlackRock to manage portfolio, understand risk exposure, navigate volatility, and market and support the trading procedures during the period January 1<sup>st</sup>, 2023 to December 31<sup>st</sup>, 2023. It takes in trade and market data, including the purchase and sale of securities and derivatives and related receivables and payables. Aladdin creates daily transactions that are utilized by the investment department and other downstream business processes such as reporting to the client.
- SIIF: system used for the NAV determination and mandates' account statements generation.
- Soluciones: It is the System that accounting managed of investment funds

## **Investment Management Processing Services**

The following describes the internal controls of Operadora de Fondos may be relevant to the internal controls of an investment management client. The related client financial transactions typically include trading activity, realized gains and losses, income and expenses, and allocation by sector and holdings and are recorded in various reports/statements provided to clients. Provided with this description is a summary of those controls to be applied by the investment management client to help ensure the system functions as contemplated in their design. As computer processing plays an integral role in the overall control environment, the description of general controls over information systems (see Information Technology Controls section) should be reviewed in conjunction with this section.

## **New Account and Account Maintenance**

When a client decides to manage their investments with Operadora de Fondos de Inversión, there are many pieces of information that must be collected before the account can be invested. This information is captured in the Client Investment Guidelines letter and the

Investment Manager must adhere to it, as the investment objectives and investment policy to follow by the client is set in the abovementioned document.

The Investment Committee is responsible of reviewing the Client Investment Guidelines letter provided by the client in order to verify if the desired objectives in terms of returns, risks and assets are achievable and available in the other market; if not, potential changes and feedback is informed to the client according to the desired objectives. Additionally, the Investment Policy Guidelines will be reviewed by the Investments Department at least annually, to check if updates or modifications are required if the desired objectives of the client have changed. Once the Investment Guidelines are approved, the Investment Management Agreement (IMA) document is reviewed by Legal, Compliance Departments and key heads of the business that are involved in the daily operation of the mandate. If no comments or changes arise, this is signed by the legal representatives of the client and Operadora de Fondos de Inversion as well.

New client investment objectives and restrictions are clearly documented, communicated and codified within Aladdin system by the Financial Risk Department to prevent unauthorized transactions. A Client Profile is created for the dissemination of information to the various personnel to maintain and trade the client's portfolio. If any client investment objectives and restrictions changes arise these are properly documented and communicated by email to the Relationship Management to prevent unauthorized transactions.

The Client OnBoarding Department will then perform the following:

- Send a notification to affected business partners that the Client Profile is available.
- Keep affected business partners updated on progress, delays, or anticipated funding dates, and send an email when the account has funded.
- Coordinate a meeting with all appropriate departments prior to funding.
- Coordinate the investments agreements with Legal and all relevant parties.

## **New Security Setup and Maintenance**

As a part of the Equities, Fixed Income and publicly traded Real Estate Portfolio Management process, new securities such as Initial Public Offering equities (IPOs), auction of government securities (M Bonds and CETES) or Corporate Securities come to market, must be analyzed for purchase. Before a security can be purchased in the trading systems, it is registered in the securities master file (SMF). To do it, the Investments Department needs to create a dummy security in the SMF and then the Operational Risk Department will be responsible for reviewing the following, but not limited to security name, maturity dates, value and if applicable the International Securities Identification Number (ISIN). Once security market information is available one day after its creation in the SMF, the security will be ready for being operated. The SMF contains qualitative data about each security owns and, also the SMF as part of Aladdin system, every time an event updates the information of the securities

this will also be updated in Aladdin for its operation. For the securities managed through SIIF system, the additions and amendments are manually performed.

Access to the SMF is restricted to authorized users within the Financial Risk Department and also is programmed to restrict the ability to add or change securities to only authorized individuals. Changes are required to go through the change management processes (IT and/or Business approval process), documentation and presentation to the appropriate group before migration to a production environment.

## **Trade Processing**

All investment transactions are authorized by the Investments management of Operadora de Fondos de Inversión, as well as reviewed by the corresponding trader or the Portfolio Manager. For each account type, Investments Department has authorized certain Portfolio Managers to approve purchases and sales for the applicable Client Accounts. Furthermore, the Financial Risk Department is responsible for validating that each operation is executed in compliance with the guidelines defined within the Investments Agreements.

For any of the Investment Agreement transactions, the Investments Department has the attribute to make purchases and sales on behalf of the applicable Client Accounts. In addition, certain affiliate clients may authorize trades to the Investments Department trading platforms for execution.

## **Securities Trading**

On a daily basis, the Financial Risk Department is responsible for performing a review which is intended to identify any discrepancies with the IMA guidelines, directions and details for any client-directed brokerage arrangements set in Aladdin system by the Investment Department and the actual trading execution. For this review, there is a dashboard in place showing the tracking of each transaction to verify the compliance with the set guidelines in one or both of the following schemes: (1) Intradia, in which a warning alert is shown in case a transaction is not being executed in accordance with the IMA guidelines before the daily cut off at 4 p.m. and; (2) Overnight in which an operation not aligned with the IMA guidelines has been executed and this need to be notified to the Investments, Compliance and Back office Departments to follow the appropriate steps. In both schemes, any inconsistencies or compliance exception alerts are identified, investigated and resolved in cooperation with the abovementioned departments. On a monthly basis, reports are presented by the Financial Risk Department in which any exception or non-compliance situation is reported.

## **Trade Allocation**

In aggregating trade orders and allocating available securities, Operadora de Fondos de Inversión provides fair and equitable treatment to all clients. The fairness of a given allocation depends on the facts and circumstances involved, including the client's investment criteria and account size and the size of the order. Operadora de Fondos de Inversión aggregates trades to give clients the benefits of efficient and cost-effective delivery of investment management processing services. By aggregating trades, more favorable executions and lower broker commissions may also be obtained. Traders have the ability to trade as a block or aggregate orders, based on orders sent to the desk and relevant market conditions.

Trades can either be conducted as a block or as series, whereby shares are systematically allocated to portfolios on a pro-rata basis in which the cost of shares is averaged out to provide client portfolios with equal treatment and service. In some cases, a fair and equitable manner may require a non-pro-rata allocation; factors such as the portfolio's guidelines, the portfolio composition, tax considerations and the risk tolerance are considered when considering a non-pro-rata allocation.

## **Best Execution Review**

On a weekly basis, the Operational Risk Department reviews a sample of the trades conducted by the Investment Department in order to validate the best execution practices. Calls are obtained from the recording system (TEAC in Business-as-Usual situation or from AVAYA in case of remote work), The calls are reviewed to validate that the trade has been done according to the statements in the local Investment Manual (Section 2 "Investment Process" – 2.2 "Investment Execution"). Some aspects validated are:

- The existence of at least two quotes
- Transactions are executed at the best price and/or market rates
- The lapse time between the quote and agreement is no longer than 30 minutes.

For this review, the Operational Risk Department downloads an Aladdin system report with the trades to validate, with this report they feed the file "Monitoreo BEP" which includes the historical validations. Subsequently, a sample of calls are reviewed through the recording system, validating Best Execution practices.

The Operational Risk Department monthly reports to the Investments Department and to the Norms Comptroller the results of the above-mentioned reviews, including observations of operations, issues regarding Best Execution (if applicable), as well as improvement opportunities. If any relevant situation is detected, the Operational Risk Department immediately informs the Investment Department and the Regulatory Controllershship, or the IT Department if it is a problem with the recording system. In addition, the summary of this review is presented to the Risk committee on a quarterly basis.

The Operational Risk Department verifies on daily basis the functionality of the phone extensions registered in TEAC or AVAYA. Issues and/or failures detected are investigated and resolved. The evidence of this control of monitoring is done by an email sent to the IT and Investment team.

## **Trade Settlement Procedures**

Before settling mandates executed operations in Aladdin system, the Custody Department is responsible for confirming that the information of each operation set in the system is aligned to the indicated in the counterparties confirmation letter, which is sent by email to a generic Treasury mailbox . In case differences arise, these are investigated; first from Operadora de Fondos de Inversión by the Investments and Custody Departments. It is important to note that from the Custody Department the operation is reviewed by two different users of the department), and then if it is the case, with the counterparties Backoffice which will inquiry about the root causes of the differences and, if applicable, send the updated confirmation letter to the abovementioned mailbox. Once the information is accurate, the Custody Department confirms the settlement in Aladdin. Aladdin system also has the functionality of generating a letter confirming the accuracy of the operations; however, this confirmation is only managed internally. Moreover, monitoring dashboards have been developed to help following up the performance of the process.

For those traded positions related to mandates contracts managed in SIIF, there is an interface from Aladdin system in which flat files are generated, subsequently imported and reconciled on a daily basis with SIIF in order to update the portfolio information.

## **Valuation**

Invested equities of Client Accounts are priced on a daily basis. PiP is the vendor that Operadora de Fondos de Inversión uses for equities valuation. This vector of prices works through and an interface with Aladdin system; every night the interface starts running so the value of all the operations recorded in Aladdin is up to date.

On an annual basis, tests are conducted by the Financial Risk Department to verify the accuracy between Aladdin and PiP prices, with a variance margin of +/- 5%. In case of greater variances, these are reviewed in cooperation with PiP and also discussed during the Risk Committee.

## **Investment Income & Corporate Actions**

Mandatory and voluntary corporate actions, including cash dividends, stock dividends, stock splits, collateral, and margin variation calls, are required to be notified by the custodian prior to being executed for local Business awareness. For voluntary operations, the Custody

Department notifies the Investments Department to conduct an analysis over the different proposed schemes such as cash or stocks and make the best decision for better return of investments. It is important to mention that there is an established period for executing the operation, so in case there is no response from Investments Department, the operation will be executed under the default set scheme. Then, once the operation is ready to be executed in Aladdin system, the Custody Department will send the response through the Custodian applicable system; one authorized user uploads the response and another one approves it to avoid any Segregation of Duties conflict. There are some cases in which the Custodian is notified by email, but this depends on each Custodian requirements. For mandatory operations, Investments Department will also be notified for its awareness and the operation is confirmed as abovementioned.

## **Reconciliations**

On a daily basis, the Custody Clerk performs two reconciliations with the information recorded in Aladdin system, SIIF and the custodian portfolio.

For the first reconciliation, the Accounting Department generates a file called MTP with the detail of the charges of each fund included in SIIF system and then uploads it to the Aladdin system through an interface. It is important to mention that this reconciliation is done automatically within Aladdin in the "Positions-Solutions Reconciliation" module; in case variations arise, the system will show them through alert notifications so that the Custody Department can proceed with the resolution. For the second, the Custody Department downloads the custodian portfolio in an excel file and also generates a report with the information of the Positions in SIIF to reconcile them in Excel, keeping the working paper and the results. In both cases, if differences arise, these will be notified to the Custodian Manager for his knowledge and the Custodian Department will proceed with the investigation and resolution. On a daily basis, trustee reconciliations are distributed via email as a sign off.

## **Client Reporting**

Client reports within the scope of this examination are defined within client's IMA and generated per frequency requirements within the IMA.

On a monthly basis, Client Accounts Statements are generated from SIIF system. In addition, the Financial Risk Department sends information daily such as benchmark and performance that are added to the client Account Statements. These are reviewed monthly by the Financial Risk Department in conjunction with the Custody and Accounting Departments, checking performance related statistics and if any issues are identified, corrections are made prior to issuance.

Once the Client Account Statement has been completed, the Operational Risk Department is responsible for sending to the Client Service Advisor and then to the client through the corporate email.

The Client Account Statement includes a listing of detailed holdings and transactions, portfolio and benchmark level performance, securities characteristics, total market value and the earned income generated from the transactions.

It is worth mentioning that there are some clients that do not require an Account Statement; instead, there are additional reports that need to be issued in the frequency and presentation that the client requires through the IMA. For these cases, the Operational Risk Department is not responsible for sending the reports to the client; nonetheless, it will review them to ensure there are no errors before issuing the reports by the Funds Accounting Department.

## **Privacy Program**

Operadora de Fondos de Inversión recognizes the importance of privacy and confidentiality of customer information and is committed to maintain customer confidence in the ability to safeguard and protect access to all entrusted information.

Previously, the Legal Department made efforts to reinforce privacy notice practices to preserve the safeguarding of sensitive information for all data subjects. In addition, Operadora de Fondos de Inversión has a Data Privacy Office whose objective is to ensure proper handling of information in compliance with applicable laws, limiting access to data and regularly testing security technology. In the course of business, it is necessary for Principal Mexico to accumulate, record, store, process, transmit and otherwise handle sensitive customer, employee, and Company information. The Company takes these activities seriously and seeks to provide fair, secure, and appropriate handling of all information. All data handling activities by Principal are intended to be consistent with all applicable local legal requirements in the jurisdictions where Principal does business. Access to information is restricted to those who have a business need to access the information to perform their job duties. All employees are expected to comply with privacy and confidentiality practices with respect to Company information. All employees are regularly reminded of their responsibility to maintain the privacy and confidentiality of all information. All employees are required to maintain the confidentiality of customer information as defined by corporate policies established by Principal. It is important to mention that the Corporate Privacy Policy which is readily available on the Company's internal website to all employees, will be the baseline for the development of the abovementioned manual, considering not only the main objective of safeguarding privacy information, but also the compliance with the Mexican data privacy regulation (Ley Federal de Protección de Datos Personales en Posesión de los Particulares, LFPDPPP). Privacy procedures for Principal processes including, but not limited to, the following:



Employees are subject to disciplinary action if they fail to report any non-compliance occurrence in accordance with the Corporate Privacy Policy.

Additional information regarding the Privacy Policy can be viewed online at [principal.com](https://www.principal.com/privacy-policies) (<https://www.principal.com/privacy-policies>).

## **Business Continuity Program**

Operadora de Fondos de Inversión is committed through the Business Continuity Program to protect its customers' financial assets and other interests. Business Continuity works toward enabling the continued operation of the different areas through an organized recovery program. Critical business capabilities and processes are identified, followed by the development of appropriate response and recovery plans. There is a local Business Continuity Policy which includes standards, roles and responsibilities and the business continuity plan (BCP). This is published and available for all the employees on the Company's intranet. The policy, roles and responsibilities, standards and plan are reviewed at least annually or every time an important amendment occurs. The Business Continuity Program in Principal (Operadora de Fondos de Inversión), is based on the Principal Corporate program, developed under professional practices, and aligned with standards such as NFPA 1600 Standard on Disaster/Emergency Management and BC Programs, ASIS International 12009, BSI 25999 and ISO22301.

The business continuity philosophy at the Company is to take an all-hazard approach, planning for the potential loss of people, facilities, and computing technology regardless of the cause for the loss. The Company also assumes, for planning purposes, the total loss of the operational site. With plans in place using this approach and assumption, it can adjust the plans to deal with less catastrophic events.

In the event an incident would affect the facilities, an enterprise-wide recovery plan is in place for the relocation of critical business capabilities to an alternative worksite. Business capabilities and processes are considered critical during the first 48 hours of an incident and are identified and prioritized via a formal Business Impact Analysis (BIA) process. Process owners are responsible for planning the continuity of their operations. The process owners define business critical processes which are then appointed to the Operational Risk Department responsible for the development, maintenance, implementation, and exercising of the business continuity plan.

Every year, as part of the Business Continuity exercises, each operative area generates a report in which the testing results are informed, as well as the identification of actions that can be required to improve the program and events' responses. The Operational Risk Department participates as sponsor of this activity.

Also, a testing is conducted over the Business Continuity Plan, throughout the year, some business continuity exercises are conducted to enable the most effective response during a business interruption. Practicing a recovery team's response helps to ensure preparedness in both the solution and the personnel during a real incident. Business continuity exercises are conducted annually and consist of the following:

- Call tree
- Alternate worksite or Remote work
- A tabletop exercise with the business area recovery team

Additional details of the Business Continuity Program are the following:

**Business Impact Analysis:** At least once a year, the Operational Risk Department meets with each process owner to review their processes and risks that may impact the operations continuity. Each department is ultimately responsible to measure and manage the risks associated with its business activities. It must understand and take an enterprise-wide view of risk, which requires an understanding of the impact of its decisions and activities may have on the whole organization. The BIA is conducted annually at a business area level. The purpose of the BIA is to review the business areas' capabilities, processes and identify their supporting applications. Based on the operational risk for that business area, recovery time objectives are identified for each area capability and supporting processes. Supporting applications are also assigned a recovery time objective, as well as a recovery point objective.

**Incident Response Framework:** There are several steps from the time an incident is identified until it is resolved. These are generally progressive; however, they may occur simultaneously depending on the nature of the incident. Communication and assessment will occur throughout the life cycle of an incident. The incident management framework provides processes, tools, and accountabilities to identify emerging and active threats to the business, mobilize a response, and mitigate the impact on the Company's people, customers, assets, resources, market share and reputation, by detecting, assessing, managing and reviewing the root cause and the impact that the incident may cause.

There are different business responsible to response to incidents within the different organization levels such as: Operative Staff, Process Leaders, Department Directors, and Local Executive Committee Leaders (CEL), performing the roles and responsibilities defined in the roles and responsibilities document.

Operadora de Fondos de Inversión has established operational response departments to deal with these incident types:

- Operative
- IT

- Cybersecurity
- Privacy
- Site and Personnel
- Fraud
- Reputation
- Business Continuity & DRP

Each incident type has its own response criteria based on its nature and severity level; nonetheless, incident escalation must follow the appropriate standards considering the estimated impact levels as shown below:

The incident severity levels are 0 – 1 and 2 – 3, in which 0 – 1 is the most severe and 2 – 3 the least severe.

**Severity Level 0 – 1:** Severe incident is defined as the one that significantly affects or stops the operation flow of Principal (Operadora de Fondos de Inversión) or that imply a potential severe event that compromise the client, employee or business sensitive information and could potentially result in a regulatory, legal, or reputational issue. Note that all Severity level 0-1 incidents must be escalated to the involved Executive Committee leaders. Moreover, these types of incidents are periodically reported to the Corporate Risk Department by the Operational Risk Department. In the event of a severity level 0-1 incident, BCP statements and measures will be considered if applicable.

**Severity Level 2 – 3:** Minor incident with a low impact, generally affects a small portion of customers and may affect with low regulatory and reputational impact. The response for these incidents could be managed by the Process Leaders and if it is the case, by the Department Directors.

Most escalation begins with the operational staff, who should notify their Process leader, Department director and in the most severe cases, these should be escalated to the Executive Committee Level.

Operadora de Fondos de Inversión also has in place the Procedure for Managing Incidents, which provides the guidelines to safeguard the clients and shareholders' interests. The maximum authority level that this procedure has is the Chief Risk and Compliance Officer and it is also approved by the Local Executive Committee.

## **Disaster Recovery Program**

The Disaster Recovery program complements the Business Continuity program focusing on IT systems recovery required to support business operations and to help ensure that recovery plans and exercises position the Company to effectively respond to incidents that

may lead to a business interruption. Reducing operational and financial risk is a key component in both programs along with creating a better prepared response department.

The Infrastructure Systems Department provides oversight for the Disaster Recovery program. The local CIO is accountable for helping ensure recovery of the business area applications and for ensuring recovery of the infrastructure systems.

The Infrastructure Systems Department is responsible for planning and implementing recovery solutions. Currently, the Company has an architecture program that helps to recover 100% of the information archived in the Triara Data Center. The response of this process allows to obtain replicated data, on a daily basis, from the production data center to the Disaster Recovery Data Center for backup and to guarantee the continuity of the infrastructure/applications in case of loss of the production data center.

Additional details of the Disaster Recovery Program follow:

**Disaster Recovery Testing:** Critical infrastructure and applications must be tested on an annual basis.

**Disaster Recovery Strategy:** The cornerstones of the Disaster Recovery strategy include two geographically distant data centers, a Production Data Center (Triara), and a Disaster Recovery Data Center. The Production Data Center is highly redundant, including redundant electrical systems, cooling systems, and uninterruptible power systems. The production data center provides high-availability solutions to mitigate the loss of a single storage or server system and the disaster recovery data center is a clone of the production data center to mitigate the loss of an entire data center through daily replication process.

## **Information Security Program**

A formal business Information Security Program has been established to help ensuring the protection of the information assets of Operadora de Fondos de Inversión. Locally, the Chief Information Officer (CIO) and the Information Security Officer are responsible for the Company's information security program. It is important to mention that there is a Corporate Security Department which supports the execution of the program's strategy for attention of events or key situations.

Currently there are policies and controls that are aligned with the NIST standard, the 800-53 framework and the Cybersecurity Framework, seeking compliance with Corporate Policies and standards, since the objective is to standardize this process among the different countries in which the Company does business.

The Information Security Program establishes policies, standards, and procedures to support the information safeguarding. Annually, the program is presented to the CIO for approval and the Information Security Department to provide guidance on how to configure security components and logical security controls. Locally, an information Security Committee is held on a monthly basis, in which the main operative areas of the business participate. Also, on a quarterly basis, the CIO participates on the Boards of Directors in which the information security topics and issues are reviewed.

Likewise, there is a quarterly Compliance report in which key information security metrics and deviations are informed, as well as the improvement opportunities and other concerns for the servers and workstations tools so these can be followed up and monitored to enhance and strengthen the process. This will help to ensure that all the departments are committed to monitor and comply with this practice.

In addition, there is another monthly report sent by the Corporate Information Security department in which all metrics, issues, and information requirements for different proposes (audits, reviews, etc.) by country are informed.

Operadora de Fondos de Inversión understands the importance of privacy and the confidentiality of customers' information. In compliance with applicable laws, a written, comprehensive security program is in place, and it applies to information stored and processed within the Company. The high- level components of the program include:

1. Risk management: which has three main initiatives:
  - a) Security risk assessment: there is a process called IT Risk Project in which corporate supports new initiatives or applications that the business requires. Locally, only the routing of requests is addressed and guided.
  - b) Third-party security profiles: it is a process that consists of a questionnaire through IRQ (Initial Risk Questionnaire). If the four questions get an affirmative answer, the third-party/external will require a review by Corporate and then the result is registered in IT GRC (information security tool). This will allow to define action plans and follow up any issues or improvement opportunities that are identified.
  - c) Development of a risk assessment framework: in which the Operational Risk Department is intended to identify potential risks that may compromise the information security in the different operative areas and to develop actions to mitigate them.
  
2. Cyber defense operations and incidents:

- a) Threat intelligence: Our Corporate has a threat intelligence department which provides a service for monitoring potential threats to create awareness and understanding of potential cyber adversaries from different sources. There is a portal that reports cybersecurity news and events for managing these situations.
  - b) Threat detection & response: There is Corporate Cyber Defense Department which is responsible for monitoring the network to identify and report suspicious activities within the operation flow of the different departments. If security incidents are identified, the Corporate Cyber Defense Department will require the local Support Center assistance to investigate or format the computer equipment if necessary. In case an incident is identified locally, this must be immediately informed to the Corporate.
  - c) Vulnerability tests: These tests are performed in two ways (1) There is a vulnerability scanning tool administered by the Corporate. Locally, vulnerability findings are managed by the Security and System Infrastructure Departments; however, in case these findings cannot be solved, these are escalated to Corporate. (2) Penetration tests are done annually by a third party in compliance with Corporate directions.
  - d) Active directory service: Corporate directory provides the list of active users as well as the management of accounts creations or deletions. Locally, the activities related to account management are limited to lock or unlock them and passwords reset.
3. Data protection: Operadora de Fondos de Inversión classifies the information into four categories: customer confidential, company confidential, internal, and public. For all these information management there are different mechanisms in place to ensure the information proper use and safeguarding such as:
- Data Loss Prevention program.
  - Monitoring tools for all the information classified as sensitive (social security numbers, software codes, credit cards, etc.) to prevent leakage of information. In case information is managed out of the organization, local Management approval must be in place.
  - Flash drives devices management through antivirus that block the use of ports and Symantec DLP to restrict writing to flash drive devices, and
  - Vulnerability: GUARDIUM tool scans the access to Oracle and SQL databases that deliver reports to Data Base Administrators (DBAs) to respond to issues that may arise. Also, Corporate reviews through the Data Active Monitoring tool in which any inadequate situation is reported.

4. Disaster recovery: managed through the Business Continuity Program (BCP) and the Disaster Recovery Program (DRP), both intended to ensure the continuity of the business considering operations and systems in case an event of loss occurs. BCP is managed by the Operational Risk Department whereas DRP by the Systems Infrastructure Department.
5. Security Education and Awareness Training: training efforts are being made to generate awareness of information security to new and active employees. Locally, new employees are trained through the Onboarding course which not only considers Company's overview, but also information security aspects.

For active employees, there is also an annual training update regarding information security topics. Also, Operadora de Fondos de Inversión has security courses at least every quarter. Furthermore, the Local Security Department sends communications at least once in a month.

Moreover, phishing simulations are performed to all employees, two per quarter totaling eight simulations per year. Phishing recognition and reporting skills are tested during these simulations. Employees who fail multiple times must complete an additional course.

The Information Security Officer is intended to provide guidance, training, and support for all employees with the purpose to remind the Company's best practices, policies updates, and to highlight hot topics related to information security considering the abovementioned.

## **Record Retention Policy**

Operadora de Fondos de Inversión retains records of information created for the ordinary course of the business for established periods, either to comply with legal regulations or to meet business requirements.

Operadora de Fondos de Inversión manages the information and data retention process through Records Retention Matrices for each operative area which are responsible for defining what type of information as well as the time of retention must be considered. The matrices include the following, but not limited to information type, managers, areas, or subareas in charge, retention time and applicable regulations. The Records Retention Matrix reflects business, legal, and regulatory retention requirements. If legal retention periods are defined for the record's subject matter, this period is the minimum time that the Company will retain the record. The responsible operative area for this record may evaluate the time period to meet business needs. These decisions are captured in the Records Retention Matrix as well.

All employees are responsible to properly retain records, consistent with this Records Retention Policy, and are required to general trainings in which they obtain the instructions about retention of information. Employees who are concerned that there is a potential violation of the Records Retention Policy, should discuss the situation with a leader/manager. The leader/manager should review the concern and report the situation. If the concerns continue, the violation is escalated to the Compliance area.

The administration and safeguarding of the matrices are in charge of Data Protection Office. The communication of the Policy and the Records Retention Matrices review, communication and verification is Compliance; however, the maintenance, updates and follow up is each operative area responsibility which will review the matrices annually. Currently, the Compliance Department is strengthening the Records Retention Policy, but any modifying issue regarding the retention terms for each area, it is its own responsibility of keeping it updated. In addition, the Compliance Department along with Corporate will conduct a review of the Records Retention Policy annually.

Once the retention period expires, records will be destroyed, unless there is a specific reason in which the retention period need to be extended, such as an imminent or pending legal or regulatory action, litigation, investigation, or regulatory audit. Records will be destroyed in a manner designed to protect the confidential information of the customers. These retention rules apply to the official copy of each area record. If duplicate copies are created for specific business needs, duplicate copies may be destroyed when that business need has been met. These copies do not need to be retained longer than the official record.

In the event of a document hold, retention rules would be suspended; records identified as being in the scope of the document hold must be retained until notification is given that the document hold has been released. This applies for both official and duplicate copies of the records.

## **Information Technology Controls**

The following describes the information systems environment of Principal, which includes Operadora de Fondos de Inversión, and the information technology controls surrounding its systems. Information technology controls establish the environment in which all applications are developed and processed. Therefore, the general information systems procedures have an impact on the effectiveness of controls in all applications.

### **System Development, Maintenance, Documentation and Change/Release Control**

Principal through the Information Configuration Management Policy guides development staff in the design, testing, and implementation of application and infrastructure changes.



Currently, Operadora de Fondos de Inversión does not conduct any application development or design as this is managed through the provider Finanzas y Soluciones S.C. of the soluciones system and the provider "Buffete de asesores en sistemas SA de CV" of de SIIF.

For the purposes of system development, maintenance, documentation, or change to a new program or an existing program, a documented business need must be (1) submitted by completing certain predefined and management-approved application forms, (2) supervisory oversight of development/maintenance activity, (3) various levels of testing and (4) approval by a person authorized to implement the project in the production environment. After analyzing each application development, design or change with the provider, a system test is carried out against all the programs affected by the requesting user/departmental support group with the assistance of the Information Technology personnel. Also, formal testing plans are established to direct the testing effort of the system, as well as Roll Back plan in case of an unforeseen impact on the production environment.

In any of the situations or needs that can appear, either by request of Operadora de Fondos de Inversión or by changes required by Finanzas y Soluciones S.C. and "Buffete de asesores en sistemas SA de CV", meetings will be held with the supplier to address the needs, concerns and risks that may arise in the modifications to be made in the system in accordance with the protocol or procedure of communication with the provider and with the change control administration policies or any that apply.

After testing the system, formal approval is obtained from the requester, the tester, and the TI head to indicate that the changes have been tested and are ready to transfer to production. Once the test acceptance approval has been received, the process proceeds to the next approval step performed by the assigned change and release approver(s). Version approvers confirm that all required documents are stored for those who participate in the process and are obligated to retain the information.

The Controls built into the change management should: (1) prevent the change owner from also being the change approver and (2) require multiple levels of approval based on the system. Access to the change and release approver is restricted to selected personnel. This access is provided by Business Units contacts for management approval.

**Documentation:** System and program documentation are generated during the various phases of the development/maintenance cycle by the development staff. The extent and adequacy of documentation are the responsibility of the discipline leader the feature in consultation with the system owner of the department supporting the system. Corporate policy requires the following to be included in each program documentation: (1) documented business need, (2) impact analysis, (3) test plan summary and sign-off, (4) migration plan, (5) Roll Back plan, and (6) change and release approvals. This documentation is retained.

**Infrastructure:** Because of their nature, most requests for changes to infrastructure (e.g., operating systems, utilities, and hardware) may result from a vendor upgrade, hardware changes, and major change in system design. Regardless of the nature of the change, the project follows the corporate Change Control policy. The Systems Infrastructure Department is responsible for completing most infrastructure changes or those which came from the corporate.

**Change and Release Management:** The change and release management processes are designed to (1) help minimize the risk to the production environment (computing and technology infrastructure) of Principal due to changes, (2) help ensure changes are made to meet specific business needs, and (3) document accountability and responsibility for changes to the environment. To help ensure the stability and high availability of the production environment and technology infrastructure of Principal, formal Configuration Management Policy is in place. This policy provides an overarching structure while allowing each Business Unit the flexibility to develop specific procedures to manage changes.

Separate development, test, pilot, and production environments are used for the distributed applications and management relies on the security features of various access control solutions, some of these environments are in control of the provider.

In the event emergency changes are needed to application systems, appropriate Information Technology personnel are contacted to correct the problem. In these cases, authorization procedures are essentially the same as those noted previously; however, they are generally performed after the change is implemented. Certain lead-level developers and above have been granted the authority to transfer programs directly from the test and pilot environment into production. All the emergency events need to follow the Change Management policy.

## **Physical Access Restrictions**

Operadora de Fondos de Inversión has two geographically data centers based in Mexico. The production data center, called "Triara" is located in Apodaca, Nuevo Leon; the second one is the Disaster Recovery Center, located in San Pedro Garza García, also in Nuevo Leon within the main offices building.

Access is restricted to both facilities at building entrances and doors of sensitive areas within buildings (e.g., computer rooms) using electromechanical locks controlled by proximity cards with additional restrictions.

To access to the production data center, there are some steps that the authorized personnel need to complete before getting into the data center itself. It is important to mention that currently, the only authorized personnel to access to the production data center is the Infrastructure Systems Department. First, an ID must be shown to the entrance guard to

access to the facility's yard. Then, the next guard will review the number of the authorized card that each member of the department has and give the corresponding proximity card to each one. Also, before accessing to the area in which the production data center is located, authorized personnel need to go through RFID sensors. A final registration needs to be done at the reception of the area in which the production data center is. There, the receptionist will ask for basic information, computer recording and also the proximity card access number, so the key for accessing to the final bunker is obtained. After that, the proximity card and finally the key will unlock the accesses until getting into the production data center. In case a new access either temporal or permanent is required, a form must be submitted to the outsourced facility management.

Regarding the Disaster Recovery Center, access is also controlled by proximity cards which are configured only to the Infrastructure Systems Department, as they are the only ones that can access there. In case a third party requires the access, they need to register in the reception and in the log located at the entrance of the data center and a member of the department will conduct the vendor over all its visit.

The proximity cards are maintained, administered, and controlled by the Infrastructure Systems Department. With regards to the production data center, even the physical cards are managed by the outsourced administrator, the directions for who is authorized for accessing come from the Infrastructure Systems Department. To access to the Disaster Recovery Center and to the Treasury Department, the proximity cards require additional configuration to access to each of these sensitive areas. Regarding the treasury area, the head of this department should notify the Infrastructure Systems Department any amendment that need to be updated in the cards configuration, to ensure the authorized personnel accesses are adequate. The accesses to the general areas of the building are also controlled by the proximity cards; however, these do not require additional locks.

Proximity cards are issued to all new employees. Additions or deletions to access for all card holders are formally requested through electronical forms, following all Human Resources steps for hires and terminations for the main office. For the production data center, an electronical form is also sent to the facility management, notifying the update. Terminated employees are required to return their access cards to their supervisor upon separation, so the accesses can be deleted.

To help ensure access are appropriate, a quarterly review of user access to the data centers is coordinated and conducted by the Infrastructure Systems Department.

## **Logical Access Administration**

Policies, standards, and procedures are established to provide guidance on how to configure security components and logical security controls.

Operadora de Fondos de Inversión uses a formal documented process to grant or revoke access to Company resources. Access rights to the system are based on the concept of "need for access to make operations related to business" to help ensure that authorized users have access according to their defined roles or responsibilities. Locally, there is an active directory that is being migrated to the Corporate one, through the project "Foundational" that seeks to migrate all the infrastructure to the Corporate one to be managed there.

For office 365, authentication is provided by Microsoft Authenticator. For provisioning and de-provisioning of accounts, locally, there is a process called ABC (Provisioning, de-provisioning, and changes) and consists of a request made through a form that is signed by the Department Director, to request an access when hiring, transferring, or terminating an employee or contractor. Once the Support Center receives the form, it proceeds to validate it; if no issues are identified, the form and additional supporting documentation are sent to the DBAs. In case access rights required are different or related to specific topics, the form and information is sent to the Corporate Infrastructure Department for the proper treatment. For de-provisioning, a daily interface with the human resources system occurs, notifying users by email to disable accounts.

On a monthly basis, a technical review is performed by comparing the active accounts with the Human Resources information to identify employee terminations, department transfers or role changes to update the accounts or access rights accordingly. This review is also conducted for third parties that may have access to the applications or systems.

In addition, for critical applications the "Entitlement Review" process seeks to carry out an access rights review of critical applications of the systems every six months or annually. User access rights lists are generated from each system and provided to application owners for its review and approval. If access rights changes are required, reviewers are responsible for submitting requests through the ABC process for provisioning and deprovisioning. It is important to mention that for those applications and systems with their assigned accounts that have already been migrated to the Corporate Active Directory, the process for any amendment is conducted through the Identity Management System.

Logical access to distributed application servers is controlled by Active Directory security settings. For all applications integrated or not to the Corporate Active Directory, the security for accessing must be guaranteed through different mechanisms such as automatic blocking due to inactivity, individual domains, among others.

## **Computer Operations**

**Incident Management:** A formal incident management process has been established for information services to track, manage, escalate, and resolve incidents (for example, disruptions in information technology) and report summary results. This process manages incidents that affect a user or a large number of users. When identified, incidents are

recorded in an incident management tool and the staff monitors open incidents for timely resolution and closure. This is achieved through a Ticket number which will help to manage and verify the response given by the Mexico support center. In addition, the incidents are assigned with a severity level based on the risk and impact that these may have. In case the incident is not that severe, the local Support Center will manage and close it, whereas a severe incident, is escalated to the Infrastructure Systems Department to evaluate the situation and if there is no local solution, the incident will be reported to the headquarters in the United States. With regards to the incidents associated with Corporate servers, communication equipment, among others, the incident notification occurs through a form sent via email to IS TECH OPS OPERATORS, (DLISTECHOPSOPERATORS@exchange.principal.com) notifying the event so they can generate the number of incident and problem for the proper follow up.

The main objective of the abovementioned, is to minimize the impact on business operations that the incidents may cause, by giving response to them as quickly as possible and identify the root cause to minimize the occurrence.

Furthermore, Operadora de Fondos de Inversión actively monitors the system and information processing to identify any potential incidents.

**System Backup:** Operadora de Fondos de Inversión policies require all servers to be backed up to provide for: (1) the recovery of processing in the event data is corrupted or lost, (2) compliance with legal, regulatory, and contractual recordkeeping requirements, and (3) the recovery of data in the event facilities are lost. This requirement is met through electronic vaulting to data center virtual tape libraries.

## **Complementary User Entity Controls (CUECs)**

The administration of the funds is the responsibility of Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos de Inversión y Principal Grupo Financiero, therefore no additional controls that clients must have in place to complement the Investment Management Processing Services and Information Technology controls are described.

## Section IV – Description of Control Objectives, Controls, Tests and Results of Testing

### Overview of Internal Controls

In planning the nature, timing, and extent of our testing of the controls specified by Operadora de Fondos de Inversión control environment, risk assessment processes, information and communication and management monitoring procedures we considered the procedures for testing as follows:

**Procedures for Assessing Completeness and Accuracy of Information Produced by Entity (IPE):** for tests of controls requiring the use of IPE, procedures were performed to assess the reliability of the information, including completeness and accuracy of the data or reports, to determine whether the information can be relied upon in the examination procedures.

Based on the nature of the IPE, a combination of the following procedures was performed to address the completeness and accuracy of the data or reports used:

- Inspection of the source documentation relating to the IPE.
- Inspection of the query, script, or parameters used to generate the IPE.
- Agreed data between the IPE and the source.
- Inspection of management's procedures.

**Controls Testing:** On the pages that follow, the description of control objectives and the controls to achieve the objectives have been specified by and are the responsibility of Operadora de Fondos de Inversión. The testing performed and the results of tests are the responsibility of the service auditor. The internal control environment was considered in planning the nature, timing, and extent of these tests.

## Investment Management Processing Services

### 1. New Account and Account Maintenance

**Control Objective:** Controls provide reasonable assurance that new accounts and modifications to existing accounts are authorized and set up in accordance with client instructions and guidelines in a complete and accurate manner.

No.	Key controls specified	Testing Performed	Results of Testing
1.1	Investments Agreements signed by both, authorized Representatives, and the client.	EY requested a sample of IMAs created during the period January - December 2023, However, based on the meetings held with the Company, no IMAs were created during the audit period.	No deviations were noted. During the examinations period, no IMAs creations were identified.
1.2	New client investment objectives and restrictions are clearly documented and codified within Aladdin system by Financial Risk Department to prevent unauthorized transactions.	EY requested a sample of IMAs related the new clients created during the period January - December 2023. However, based on the meetings held with the Company, no IMAs were created during the audit period.	No deviations were observed. During the examination period, no IMAs related to the creation of new clients were identified.
1.3	If any client investment objectives and restrictions changes arise these are properly documented and communicated by email to the Relationship Management to prevent unauthorized transactions. Performed changes must be reviewed and approved by the appropriate personnel avoiding Segregation of Duties (SoD) conflicts.	EY confirmed that there were no changes to the investment objectives and restrictions requested by the client in the existing IMAs, Additionally, the monthly performance report of executed transactions was reviewed.; In case of any requested change not reflected in the transactions included in the report, these are identified and clarified.	No deviations were observed. During the examination period, no changes in investment objectives were identified.

## 2. New Security Setup and Maintenance

**Control Objective:** Controls provide reasonable assurance that new securities and changes to existing securities are established in the security master file system and reviewed in a complete, accurate and timely manner.

No.	Key controls specified	Testing Performed	Results of Testing
2.1	A request for a new security is initiated by a Portfolio Manager and directed to an email address for the Operational Risk Department which is responsible for building and maintaining the Securities Master File (SMF). After the security is built in SMF by the Investment Department, the Financial Risk Department reviews critical and manual fields for accuracy.	EY obtained and witnessed the pulling of a system-extracted report with the new Security Instruments and for a sample of new securities, we inspected the documentation noting the following: <ul style="list-style-type: none"> <li>- The Security Instruments are requested by the Portfolio Manager.</li> <li>- The Security was built appropriately in the Security Master File from Aladdin System by Operational Risk Department.</li> <li>- Evidence of the Financial Risk Department review.</li> </ul>	No deviations noted.
2.2	Daily, dashboards are generated in order to keep track of any identified exception and are monitored by the Financial Risk Department.	EY performed a walkthrough with management and inspected evidence of the functionality of Aladdin Dashboards to flag exceptions to be researched and resolved by a member of the Financial Risk Department.	No deviations noted.
2.3	Aladdin System is programmed to restrict the ability to add or change securities in the SMF and the performance dashboards only to authorized users.	EY requested the access rights configured in Aladdin for adding or changing securities in the SMF. We also validated that the users listed in the access rights authorized user list, matched with the parameters set at a user level permission.	No deviations noted.



### 3. Trade Processing

**Control Objective:** Controls provide reasonable assurance that investment transaction instructions are authorized, executed, and entered into the system in a complete, accurate and timely manner.

No.	Key controls specified	Testing Performed	Results of Testing
3.1	The Investments management has the authority to initiate orders to buy or sell approved securities in Aladdin system.	EY walked through the system functionality and verified that there is only one group of authorized employees to buy or sell approved securities. Then, we confirmed with management that the access rights were properly assigned. Additionally, we obtained the screenshots at a user level with the listing of permissions in the system for those users in the group, to confirm our first validation.	No deviations noted.
3.2	For client restrictions codified in Aladdin system, a pre-trade/transaction compliance check is automatically run prior to execution. Pre-trade compliance exceptions are identified in real-time, tracked, and resolved prior to the trade being executed.	EY performed a walkthrough with management and inspected evidence of the functionality of client restrictions codified in Aladdin System. Additionally, the generation of exceptions was observed, which are investigated and resolved.	No deviations noted.
3.3	Compliance exception alerts are identified prior to settlement, tracked, and resolved within the same day by the Portfolio Managers. Exception reports are generated daily and are reviewed by the Financial Risk Department.	EY performed a walkthrough with the management team to review the operational effectiveness of the Aladdin system. It was observed that the system generates prior settlement alerts for compliance exceptions. These exceptions are then thoroughly investigated and addressed by a member of the Financial Risk Department.	No deviations noted.
3.4	On a monthly basis, the Investment Committee is responsible to approve the trading strategy and the investment portfolio over the mandates positions by attending the Committee monthly meeting which follow-up is agreed and documented in memos to confirm the best trading results.	EY confirmed that monthly and daily meetings are held in which the trading strategy and investment portfolio are discussed, reviewed, and approved on the positions of the mandates by the Investment Committee; Therefore, a 2-month sample was generated, in order to verify the monitoring of the negotiation strategy and investment portfolio.	No deviations noted.

No.	Key controls specified	Testing Performed	Results of Testing
3.5	Trade errors are properly documented and resolved by the Portfolio Managers. Changes necessary to prevent future recurrence are adopted.	EY performed a walkthrough with management and inspected evidence that when trade errors occur, these errors are resolved by the Portfolio Managers and changes to prevent future recurrence are adopted.	No deviations noted.

#### 4. Securities Trading

**Control Objective:** Controls provide reasonable assurance that portfolio guidelines are monitored, and exceptions are identified and resolved in a complete, accurate and timely manner.

Since the Securities Trading Process control objective and associated risks are covered by the controls defined for the Trade Processing Process, additional testing was not conducted.

No.	Key controls specified	Testing Performed	Results of Testing
4,1	For client codified restrictions in Aladdin, a pre-trade/transaction compliance check is automatically run prior to execution. Pre-trade compliance exceptions are identified in real-time, tracked, and resolved prior to the trade being executed.	EY performed a walkthrough with management and inspected evidence of the functionality of client restrictions codified in Aladdin System. Additionally, the generation of exceptions was observed, which are investigated and resolved.	No deviations noted.
4,2	A warning is issued in Aladdin when pre-trade/transaction compliance issues are identified.	EY performed a walkthrough with management and inspected evidence of the Aladdin system's functionality, observing that a warning is issued when compliance issues are identified pre-trade/transaction.	No deviations noted.
4,3	Compliance exception alerts in Aladdin are identified prior to settlement, tracked, and resolved within the same day by Financial Risk Department. All breaches are properly resolved and disclosed, if material, to the relevant clients in a timely manner. Necessary changes to prevent future reoccurrence are adopted. Dashboards are generated daily and are reviewed by Portfolio Managers.	EY performed a walkthrough with management and inspected evidence of the functionality of Aladdin Dashboards to flag exceptions to be researched and resolved by a member of the Financial Risk Department.	No deviations noted.
4,4	On a monthly basis, the Operations Risk Department certify compliance with client investment objectives and restrictions for equity and fixed income accounts.		No deviations noted.

No.	Key controls specified	Testing Performed	Results of Testing
		EY generated the sample for the certification of compliance with client investment objectives and restrictions for equity and fixed income accounts, considering the monthly frequency of the control.	

## 5. Trade Allocation

**Control Objective:** Controls provide reasonable assurance that block orders are allocated to clients in an equitable manner.

No.	Key controls specified	Testing Performed	Results of Testing
5.1	At least annually, the Investment Department evaluates qualitatively and quantitatively, the service levels provided by the counterparties over the mandates conditions to review the fairness of allocation process.	By inquiry with management, EY obtained the knowledge that two counterparties' evaluations were performed during the year 2023. Inspected the documentation noting the following: - No issues were identified by the Investment Department during the evaluations. - The forms utilized to execute the evaluations appear to be appropriate and complete.	No deviations noted.
5.2	Daily, the Investment Department monitors and detects any potential deviation to the allocation procedures through the Aladdin dashboards. Any identified exceptions are investigated and resolved by the Compliance Department.	EY performed a walkthrough with management and inspected evidence of the functionality of Aladdin Dashboards to flag exceptions to be researched and resolved by a member of the Financial Risk Department. No exceptions were identified during the scope period.	No deviations noted.

## 6. Best Execution Review

**Control Objective:** Controls provide reasonable assurance that Management conduct periodic and systematic review of best execution efforts.

No.	Key controls specified	Testing Performed	Results of Testing
6.1	The Financial Risk Committee is notified on a quarterly basis with the results and improvement opportunities related to the best execution efforts.	By inquiry with management, EY obtained the knowledge that the results of best execution process are presented quarterly to the Financial Risk Committee. EY inspected the documentation noting: The Financial Risk committee issues a memorandum where the agreements of meetings are documented.	No deviations noted.
6.2	When registering and codifying new Counterparties in Aladdin, these must be approved by the Investments Committee. Also, on a quarterly basis a review is conducted by the Financial Risk Department to confirm accuracy between the counterparties on the Approved Counterparties List and Aladdin system. Any identified concerns or discrepancies are investigated and resolved.	By inquiry with management, EY confirmed that no new counterparties were created during the audit period.  The quarterly review carried out by the Custody Department was validated, confirming the veracity of the counterparties in the Aladdin system.	No deviations were noted. During the examinations period, no new counterparties were created.
6.3	The Operational Risk Department verifies on daily basis the functionality of the phone extensions registered in TEAC or AVAYA. Issues and/or failures detected are investigated and resolved. The evidence of this control of monitoring is done by an email sent to the IT and Investment team	EY selected a sample of dates to verify that the review of the operation of the extensions is performed, confirming. In the case of exceptions, we obtained the corresponding clarifications and supporting evidence. No problems were noted.	No deviations noted.
6.4	The Operational Risk Department is responsible for reviewing the best execution process is documented and that there are backups to guarantee the continuity of the reviews in case of absence or turnover.	By inquiry with management, EY confirmed that there are two procedures in place regarding to the Best Execution Process (business as usual situation and business in case of remote work). EY obtained the established manuals and inspected the documentation noting the following: Both manuals entirely detail the Best Execution practices for each case appropriately.	No deviations noted.

## 7. Trade Settlement Procedures

**Control Objective:** Controls provide reasonable assurance that investments are settled, and custodians are informed of transactions in a complete, accurate and timely manner.

No.	Key controls specified	Testing Performed	Results of Testing
7.1	For every traded mandate position, counterparties confirmation letters are sent to the Custody Department emails and / or Treasury generic mailbox to perform a review over the mandates positions' information in Aladdin system and the details in the counterparties confirmation letter.	From a selected sample of traded operations, EY validated the following: - The communication between the counterparties and the Custody Department seems to be effective. - Confirmation letters sent by the counterparties and settled operations in Aladdin matched. - Approvals from the Custody Department are in place.	No deviations noted.
7.2	Unsettled or failed trades are investigated and resolved by the Custody Department.	EY obtained a system-extracted listing of the unsettled or failed trades during the scope period and for a sample inspected the supporting documentation noting the following: - The communication between the counterparties and the Custody Department is effective. - In case the root cause of the unsettlement is something outside the normal operation of the business it is documented in the signed confirmation letter. The resolution is documented as well.	No deviations noted.

## 8. Valuation

**Control Objective:** Controls provide reasonable assurance that investment prices are received from an authorized source and updated in a complete, accurate and timely manner and price overrides are authorized and processed in a complete and accurate manner.

No.	Key controls specified	Testing Performed	Results of Testing
8.4	Annual reasonableness reviews of prices provided by valuation sources are conducted by the Operational Risk Department in Aladdin through ANSER tool. In case exceptions arise, these are investigated and supported. Likewise,	EY validated the "Position and Risk Report" extracted from Aladdin ANSER tool, by comparing the prices set in Aladdin and the prices provided by PiP, the exceptions were corrected.	No deviations noted.

No.	Key controls specified	Testing Performed	Results of Testing
	the results are presented to the Risk Committee. In addition, automatic valuation is done through an interface between Aladdin and the price vector "PiP".		

## 9. Investment Income & Corporate Actions

**Control Objective:** Controls provide reasonable assurance that investment income, corporate actions, collateral, and margin variation notices are identified and received from an authorized source and are updated in the system in a complete, accurate and timely manner.

No.	Key controls specified	Testing Performed	Results of Testing
9.1	Per event, the Investments Department performs an analysis to support the best decision-making prior executing a voluntary corporate action.	Verification of the analyzes carried out by the Investment Department is carried out, to support the best decision-making prior to executing a voluntary corporate action; For this reason, a sample of eleven cases was generated for a population of 108 cases identified during the evaluated period.	No deviations noted.
9.2	For voluntary actions, the confirmations are done through the Custodian system or email. For confirmations via system, one authorized user is responsible for uploading the response and a different user approves it, avoiding any Segregations of Duties conflict.	Verification of confirmations made through the Custodian system or email is carried out for voluntary actions; For this reason, a sample of eleven cases was generated for a population of 108 cases identified during the evaluated period.	No deviations noted.

## 10. Reconciliations

**Control Objective:** Controls provide reasonable assurance that security positions and cash balances reflected in investment management systems are reconciled in a complete, accurate, and timely manner to actual positions and balances held by custodians/banks.

No.	Key controls specified	Testing Performed	Results of Testing
10.1	<p>On a daily basis a reconciliation between Aladdin system and SIIF is automatically performed in the module "Conciliación de Posiciones-Soluciones". In case of any discrepancy is identified, this is investigated and solved by the Custody Department.</p>	<p>EY confirmed that the automatic reconciliations between Aladdin and SIIF systems are performed daily. Therefore, EY performed a walkthrough with management and inspected the evidence of the functionality of Aladdin to flag exceptions to keep track of them.</p> <p>EY noted that daily, the MTP file is updated with the balances of the mandate's transactions run within SIIF. To then be uploaded into Aladdin and the reconciliation can be automatically done. In case of discrepancies, these are shown by the system dashboard; then, these are investigated and solved.</p>	No deviations noted.
10.2	<p>On a daily basis a reconciliation between PortafoliosNet and the custodian portfolio is manually conducted. In case of any discrepancy is identified, this is investigated and solved by the Custody Department. Reconciliations are reviewed and approved (physically or electronically signed or via email).</p>	<p>From a sample of selected dates, EY inspected the documentation noting the following:</p> <ul style="list-style-type: none"> <li>- The daily reconciliations seem to be executed properly.</li> <li>- All the identified exceptions were identified and documented properly by the Custody Department.</li> <li>- Additionally, EY validated that the reconciliations are reviewed and approved properly by the Custody Department.</li> </ul>	No deviations noted.

## 11. Client Reporting

**Control Objective:** Controls provide reasonable assurance that client reporting and client billing are accurate, complete, and provided to clients in a timely manner.

No.	Key controls specified	Testing Performed	Results of Testing
11.1	The Operations Department generates the Client Account Statements from Aladdin system on a monthly basis. Validation is performed by the Operations Department along with the Custody and Accounting Departments and if any issue is identified, corrections are made prior to issuance in Aladdin system.	EY judgmentally selected a sample of clients with mandates positions noting the following: <ul style="list-style-type: none"> <li>- - Operations Department generates the Client Account Statements monthly timely or when the client requires it based on its established guidelines.</li> <li>- - Operations, Custody and Accounting Departments validate, identify and correct issues prior submitting the Account Statements or required reports.</li> </ul>	No deviations noted.
11.2	The Client Service Advisor distributes reports to clients on at least a monthly basis by email.	The verification of the communication issued by the Customer Service Advisor is carried out, for which one client with mandate positions is identified.	No deviations noted.
11.3	Before terminating or discontinuing earlier than agreed, final fee invoices are generated and are pro-rated to the termination date by the Operations Department.	By inquiry with management, EY obtained the understanding of the procedure of early contract termination or discontinuation. However, there were no early terminations or discontinuations during the audit scope period.  Therefore, for control documentation purposes, EY required the corresponding policy/procedure in which the early terminations or discontinuation are set to document the existence of the control.	No deviations were noted. During the examinations period, no terminating or discontinuing earlier agreed were identified.



## Information Technology Controls

### 12. System Development, Maintenance, Documentation and Change/Release Control

**Control Objective:** Controls provide reasonable assurance that:

- Application code and configuration parameter changes are initiated as needed, are authorized, and function in accordance with application specifications to (1) result in valid, complete, accurate, and timely processing and data, (2) provide for the functioning of application controls, and (3) support segregation of duties; and
- Network infrastructure is configured as authorized to (1) enable applications and application controls to operate effectively, protect data from unauthorized changes, (3) provide for its availability for processing, and (4) support segregation of duties.

No.	Key controls specified	Testing Performed	Results of Testing
12.1	The Principal Change Control Policy is used to guide development personnel in the design, testing, and implementation of application and infrastructure changes.	EY validated there are procedures in place that provide guidelines to apply changes, which are properly documented.	No deviations noted.

No.	Key controls specified	Testing Performed	Results of Testing
12.2	Eventually, the request stakeholder submits the pre-defined request form and this should be approved by the corresponding Department Lead in order to develop a new program or change an existing program.	EY selected a sample of changes submitted during the period by observing that presented in the predefined request form and approved by the relevant Department Head	No deviations noted.
12.3	System testing is performed against all impacted programs by the requesting user/departmental support group with the assistance of Information Technology personnel under a testing environment. Formal test plans are developed to direct the system testing effort.	EY selected a sample of the changes presented during the period by noting that tests were performed between user/departmental support group	No deviations noted.
12.4	Associated controls to the system change management process: (1) prevent the change owner from also being the change approver of the change and (2) require multiple levels of approval based on the system. Change and release approver access is restricted to selected personnel. This access is provisioned by Business Units contacts per approval by management.	EY selected a sample of the changes submitted during the period, verifying that the owner of the change is not the approver of the change.	No deviations noted.

No.	Key controls specified	Testing Performed	Results of Testing
12.5	<p>Following system testing, formal requester/tester sign-off is obtained from the requesting user and/or support group personnel involved in testing to indicate the changes have been tested and are ready for transfer to production. Once the test acceptance approval has been received, the change continues to the next approval step which is done by the assigned change and release approver(s). Release approvers confirm through an email that all required documents are stored for those who participate in the process and are obligated to retain the information. Emergency changes will be managed and documented according to the statements in the Change Control Policy.</p>	<p>EY selected a sample of the changes presented during the period, noting that they were duly approved</p>	<p>No deviations noted.</p>
12.6	<p>All changes or needs required in the system are monitored on a quarterly basis from the stakeholders, and these changes are selected in a sample from the transfer history report to validate the following: (1) each change was appropriate, (2) documentation was retained, and (3) the necessary approvals were obtained.</p>	<p>EY through Blackrock solutions' SOC report verified change management compliance for the Aladdin system.</p>	<p>Deviation noted. The Monitoring control that addresses to the risk to unauthorize changes, it is not to be able to SIIF and Solutions applications.</p>
<p>Management Response: As of the date of notification by EY, the SIIF and Soluciones applications will be included in the scope of control.</p>			

### 13. Physical Access Restrictions

**Control Objective:** Controls provide reasonable assurance that physical access to the data centers and other sensitive areas is restricted to authorized and appropriate personnel.

It was confirmed that BlackRock solutions manages the physical server and has control over the physical access to the datacenter. EY confirmed that Operadora de Fondos de Inversión does not have control over access to the datacenter and in case of requiring access, special authorization has to be granted by BlackRock solutions. No physical access was requested or registered during the audit period.

No.	Key controls specified	Testing Performed	Results of Testing
13.1	Access is restricted to Principal Fondos de Inversión, S.A. de C.V. Operadora de Fondos de Inversión facilities at building entrances and at doors of sensitive areas within buildings (e.g., computer rooms) using electromechanical locks controlled by proximity card, with additional configuration for sensitive areas. In the event of any security device failure, documented mitigation processes are in place.	EY evidenced that access to Principal Fondos de Inversión, S.A. de C.V. facilities is restricted at building entrances and at the doors of sensitive areas within the buildings (e.g., computer rooms) by means of electromechanical locks controlled by proximity card.	No deviations noted.
13.2	A quarterly review of users granted access to the data centers is conducted by Infrastructure Systems team.	EY selected a sample from the quarterly review of data center accesses.	No deviations noted.

No.	Key controls specified	Testing Performed	Results of Testing
13.3	Physical accesses are removed when a user is terminated. A notification is made to the Infrastructure System team so it proceeds with the update in the proximity card system to disable cards of terminated employees.	EY requested a sample of accesses revoked during the period January - December 2023. However, according to meetings held with the Company, no access was revoked during the audit period.	No deviations were observed. During the review period, no access revocation was identified.

#### 14. Logical Access Administration

**Control Objective:** Controls provide reasonable assurance that logical access to applications and data is restricted to authorized and appropriate users to protect applications and data from unauthorized modification and support the segregation of duties.

No.	Key controls specified	Testing Performed	Results of Testing
14.1	Policies, standards, and procedures are established throughout Principal information resources to establish requirements for how to configure security components and logical security controls.	EY confirmed policies and procedures are in place throughout Principal information resources.	No deviations noted.

No.	Key controls specified	Testing Performed	Results of Testing
14.2	For provisioning and de-provisioning of accounts, ABC process is conducted when the requester user sends a request form approved by the Department Head to the Support Center that validates the access request is adequate based on the job functions. In case specific access rights are needed, the Support Center notifies the Corporate Infrastructure Department for proper treatment.	EY selected a sample of users to validate the provisioning, de-provisioning, or changes of access rights process, noting this is properly supported.	No deviations noted.
14.3	A monthly technical review is performed to identify employee terminations to disable the accounts or access rights in the applications and/or systems. Third parties with granted access rights are also considered within the review.	EY observed that there is a monthly report which is the base to conduct a review over the access rights for identifying users that are no longer working in the Company. We noted that the report called: Monthly terminated review - Worker Checklist.	No deviations noted.
14.4	Accounts with no logging activity for a period longer than 90 days are automatically blocked or disabled.	EY observed the process carried out for the periodic review accounts with no logging activity for a period longer than 90 days.	Deviation noted. It was evident that control does not have scope over the SIF and Solutions applications.
		Management Response: The entity will carry out the configuration as of December 31, 2024.	

No.	Key controls specified	Testing Performed	Results of Testing
14.5	User access review is conducted at least annually by IT Department along with the Process owners for critical applications' granted access rights. If discrepancies are identified, these are evaluated to define if the access should remain or not.	EY observed that the process executed for the periodic user access review is conducted annually by the IT Department along with the Process owners for critical applications including Aladdin and SIIF, noting improper access rights have not been granted.	No deviations noted.
14.6	The Windows security parameters are reviewed on a quarterly basis by Information Security and Risk. Settings not in compliance with the defined security standards are reported to the CIO Working Group	EY requested the reports, generating a quarterly sample with the reviews carried out by Information Security and Risk.	No deviations noted.

## 15. Computer Operations

**Control Objective:** Controls provide reasonable assurance that application and system processing are authorized and executed in a complete, accurate, and timely manner; and deviations, problems, and errors are identified, tracked, recorded, and resolved in a complete, accurate, and timely manner. Controls provide reasonable assurance that data and applications are backed up to permit restoration of applications and processing in the event of the destruction of the applications or data.

No.	Key controls specified	Testing Performed	Results of Testing
15.1	Principal Fondos de Inversión, S.A. de C.V. actively monitors the system and information processing to identify incidents. When identifying incidents, the user is responsible to report the incident to the Support Center which generates the ticket and assigns it to the appropriate level based on the severity for timely response	EY validated that incidents reported by users are resolved within a reasonable period, assigned to the correct levels, and closed appropriately.	No deviations noted.
15.2	Servers are backed up and replicated into the disaster recovery data center on a daily basis.	EY confirmed that the servers are backed up daily and replicated to a disaster recovery center from the report provided, EY noted that the backups were running as scheduled and that data was available when needed.	No deviations noted.



## **Section V – Other Information Provided by Operadora de Fondos de Inversión.**

No comments reported by the entity.