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

Assurance Report on Controls at a Service Organization

(ISAE 3402) SOC 1 Type 2

June 20, 2025

The better the question. The better the answer. The better the world works.

Building a better working world

SECTION I

Independent Service Auditor's Assurance Report

Independent Service Auditor's Assurance Report on the Description of Controls, their Design and Operating Effectiveness

To the Board of Directors
Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos de Inversión, Principal Grupo Financiero
México D.F.

Scope
We have been engaged to report on Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos de Inversión, Principal Grupo Financiero description at Section III of Investment Management System, with the support of Aladdin, SIIF and Solutions, used for the registration and follow-up of investments, throughout the period January 1, 2024, to December 31, 2024 (the Description), and on the design and operation of controls related to the control objectives stated in the Description.

The Control Objectives and related controls included in the Description are those that Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos de Inversión, Principal Grupo Financiero management considers 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.

Based on our procedures, as described in section "III" of the System Description, no new investment contracts or mandates were issued by user entities during the period from January 1 to December 31, 2024. Therefore, we did not apply procedures to evaluate the operating effectiveness of controls related to control objective CO1, which states that "Controls provide reasonable assurance that new accounts and modifications to existing accounts are authorized and configured in accordance with client instructions and guidelines in a complete and accurate manner," solely with respect to control ID No. 1.1 and No. 1.3, and control objective CO6, which states that "Controls provide reasonable assurance that investments are settled and custodians are informed of transactions in a complete, accurate, and timely manner," solely with respect to control ID No. 7.1.

Additionally, no terminations of investment mandate contracts were made by user entities during the period from January 1 to December 31, 2024. Therefore, we did not apply procedures to evaluate the operating effectiveness of controls related to control objective CO10, which states that "Controls provide reasonable assurance that client reporting and billing are accurate, complete, and provided to clients in a timely manner," solely with respect to control ID No. 11.3.

The Description also indicates that certain Control Objectives can be achieved only if the controls of Principal Fondos de Inversión S.A. de C.V Operadora de Fondos de Inversión Principal Grupo Financiero are suitably designed and operate effectively, along with the related controls at the service organization.

Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos de Inversión, Principal Grupo Financiero uses carved-out BlackRock to provide the Aladdin application platform used for generating and managing information Investment Funds as a trading platform and uses carved-out Amazon Web Service to provide Infrastructure as a Service (IaaS) for the SIIF application provided as of November 18, 2024. The Description includes only the Control Objectives and related controls of Principal Fondos de Inversión S.A. de C.V Operadora de Fondos de Inversión Principal Grupo Financiero, and includes the general controls of Aladdin, SIIF, and Soluciones as systems used for operations and excludes the control objectives and related controls of carved-out BlackRock and AWS. The Description also indicates that certain Control Objectives specified by Principal Fondos de Inversión S.A. de C.V Operadora de Fondos de Inversión Principal Grupo Financiero can be achieved only if complementary subservice organization controls assumed in the design of Principal Fondos de Inversión S.A. de C.V Operadora de Fondos de Inversión Principal Grupo Financiero s controls are suitably designed and operating effectively, along with the related controls at Principal Fondos de Inversión S.A. de C.V Operadora de Fondos de Inversión Principal Grupo Financiero. Our engagement did not extend to such complementary controls of carved-out BlackRock and AWS, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The information included in Section V – Other Information Provided by the Investment Fund Operator is presented by management of Principal Fondos de Inversión S.A. de C.V Operadora de Fondos de Inversión Principal Grupo Financiero to provide additional information and is not a part of Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos De Inversión, Principal Grupo Financiero Description. Information about Privacy Program, Business Continuity Program, Incident Response, Disaster Recovery Program, Information Security Program, and Data Retention and Destruction Policy has not been subjected to the procedures applied in our engagement of the Description of the System and of the suitability of the design and operating effectiveness of controls to achieve the related Control Objectives, and, accordingly, we express no opinion on it.

Limitations of Scope 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. Record Retention Policy

Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos de Inversión, Principal Grupo Financiero *responsibilities*
Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos de Inversión, Principal Grupo Financiero is responsible for preparing the Description and accompanying statement at Section III including the completeness, accuracy, and method of presentation of the Description and statement; providing the services covered by the Description; stating the control objectives; identifying the risks that threaten the achievement of the Control Objectives, selecting the criteria presented in the statement, and designing, implementing, and effectively operating controls to achieve the stated control objectives.

Our independence and quality management
We have complied with the independence and other ethical requirements of the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants (including International Independence Standards), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

We apply International Standard on Quality Management 1, Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services engagements, which requires that we design, implement and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Our responsibilities
Our responsibility is to express an opinion on Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos De Inversión, Principal Grupo Financiero Description and on the design and operation of controls related to the control objectives stated in the Description, based on our procedures. We conducted our engagement in accordance with International Standard on Assurance Engagements 3402, Assurance Reports on Controls at a Service Organization, issued by the International Auditing and Assurance Standards Board. That standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the Description is fairly presented, and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organization involves performing procedures to obtain evidence about the disclosures in the service organization's description of its system, and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgment, including the assessment of the risks that the description is not fairly presented and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the

suitability of the objectives stated therein, and the suitability of the criteria specified by the service organization and described at Section III.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Limitations of controls at a service organization
Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos de Inversión, Principal Grupo Financiero Description is prepared to meet the common needs of a broad range of user entities and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in its own particular environment. Also, because of their nature, controls at a service organization may not prevent or detect all errors or omissions in processing or reporting transactions or identification of the function performed by the system. Also, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organization may become inadequate or fail.
Additionally, due to the nature of automated controls, the walk-through and evaluation of the controls were performed during 2024.

Opinion
Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are those described at Section III. In our opinion, in all material respects:

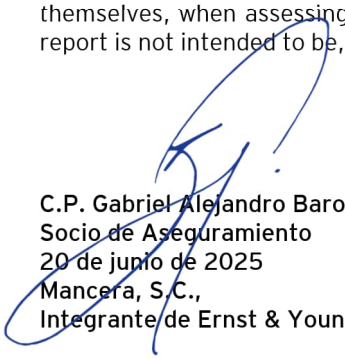
a. The Description fairly presents the Investment Management System, supported by Aladdin, SIIF and Solutions used for the registration and monitoring of investments system as designed and implemented throughout the period from January 1, 2024, to December 31, 2024.

b. The controls related to the control objectives stated in the Description were suitably designed throughout the period from January 1, 2024, to December 31, 2024, to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period January 1, 2024, to December 31, 2024; and

c. The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the Description were achieved, operated effectively throughout the period January 1, 2024, to December 31, 2024, if complementary subservice organization and user entity controls assumed in the design of Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos de Inversión, Principal Grupo Financiero controls operated effectively throughout the period January 1, 2024, to December 31, 2024.

Description of tests of controls
The specific controls tested, and the nature, timing, and results of those tests are listed on pages Section IV.

Intended users and purpose
This report and the Description of tests of controls on pages Section IV are intended only for user entities who have used Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos de Inversión, Principal Grupo Financiero Investment Management System, with the support of Aladdin, SIIF and Solutions, used for the registration and follow-up of investments, and their auditors, who have a sufficient understanding to consider it, along with other information including information about controls operated 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. Gabriel Alejandro Baroccio Pompa
Socio de Aseguramiento
20 de junio de 2025
Mancera, S.C.,
Integrante de Ernst & Young Global, Ciudad de México

SECTION II

Management Statements

Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos De Inversión, Principal Grupo Financiero Management Statements

June 20, 2025

Mancera, S.C.
Mr. Gabriel Alejandro Baroccio
Socio
Ciudad de México

The accompanying description has been prepared for user entities who have used associated with the service Investment Management System, supported by the Aladdin, SIIF, and Solutions systems used for investment registration and monitoring, and their auditors who have a sufficient understanding to consider the description, along with other information including information about controls operated by BlackRock Inc. and Amazon Web Services user entities themselves, when assessing the risks of material misstatements of user entities' financial statements.

Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos de Inversión, Principal Grupo Financiero uses subservice organization to the description of the Aladdin, Aladdin Risk, Aladdin Wealth and Investment Accounting Services System ("System") of Management of BlackRock or "BlackRock" for processing user entities' transactions and Amazon Web Service to provide Infrastructure as a Service (IaaS) for the SIIF application provided as of November 18, 2024. The Description includes only the control objectives and related controls of Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos de Inversión, Principal Grupo Financiero and excludes the control objectives and related controls of the subservice organization. The Description also indicates that certain control objectives specified in the Description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The Description does not extend to controls of the subservice organization.

Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos de Inversión, Principal Grupo Financiero confirms that:

a. The accompanying description at pages of Section III fairly presents the Attestation (examination), SOC 1 Type II based on the "International Standard on Assurance Engagements" ISAE 3402 (reasonable). This will evaluate the design, implementation, and operational effectiveness related to the service 'Investment Management System, supported by the Aladdin, SIIF, and Soluciones systems used for investment recording and monitoring,' provided by Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos de Inversión, Principal Grupo Financiero, Investment Fund Manager, and the 'Funds' to its user organizations system (System) for processing user entities' transactions throughout the period January 1 to December 31, 2024. The criteria used in making this statement were that the accompanying description:

(1) Presents how the System was designed and implemented to process relevant transactions, including, if applicable:

- The types of services provided, including, as appropriate, the classes of transactions processed.
- The procedures, within both information technology and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions were initiated, recorded, processed, corrected as necessary, and transferred to the reports prepared for user entities.
- The information used in the performance of the procedures including supporting information; this includes the correction of incorrect information and how information was transferred to the reports prepared for user entities.
- How the System dealt with significant events and conditions, other than transactions.

- The process used to prepare reports for user entities.

- Services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.

- Relevant control objectives and controls designed to achieve those objectives.

- Controls that we assumed, in the design of the system, would be implemented by user entities and subservice organizations, and which, if necessary to achieve control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by us alone.

- Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring activities that were relevant to the services provided, including processing and reporting user entities' transactions.

(2) Includes relevant details of changes to the service organization's System during the period January 1 to December 31, 2024.

(3) Does not omit or distort information relevant to the scope of the System being described, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities and their auditors, and may not, therefore, include every aspect the System that each individual user entity may consider important in its own particular environment.

b. The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period January 1 to December 31, 2024, if subservice organizations applied the complementary subservice organization controls and user entities applied the complementary user entity controls assumed in the design of Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos de Inversión, Principal Grupo Financiero controls throughout the period January 1 to December 31, 2024 The criteria used in making this statement were that

(1) The risks that threatened achievement of the control objectives stated in the description were identified.

(2) The identified controls would, if operating as described, provide reasonable assurance that those risks Control prevent the stated control objectives from being achieved; and

(3) The controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period January 1 to December 31, 2024.

Jaime Santibañez
Head Asset Management Mexico
Principal Fondos de Inversión, S.A. D
C.V.

SECTION III

Description of the Services

Description of the Services of Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos de Inversión, Principal Grupo Financiero

Scope

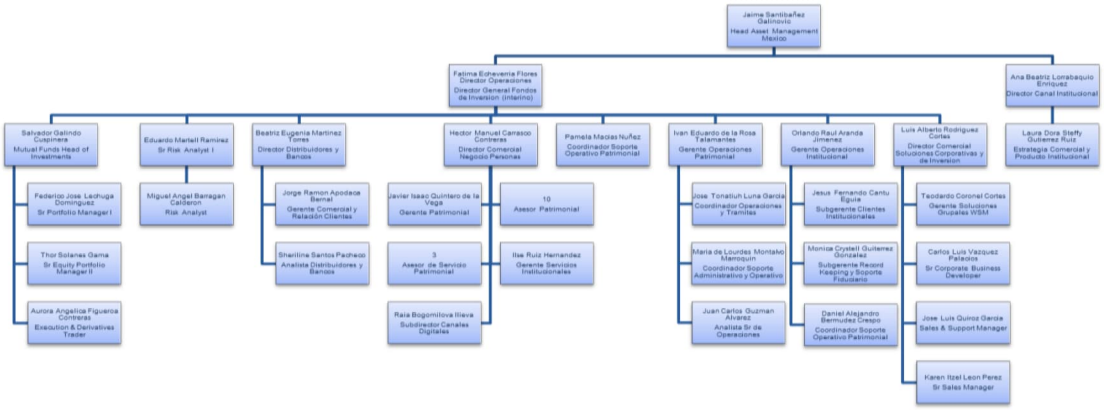
This report covers the investment management operations for institutional clients of Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos de Inversión, Principal Grupo Financiero for the period from January 1, 2024, to December 31, 2024. It does not include other affiliate operations.

Organizational Overview

Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos de Inversión, Principal Grupo Financiero is an indirect wholly owned subsidiary of Grupo Financiero Principal, which operates in Mexico primarily through three businesses: *Principal Afore* (retirement funds), *Principal Investment Funds, Operadora de Fondos de Inversión* (Investment Funds) and *Principal Compañía de Seguros* (life insurance) helping individuals and businesses plan and build their financial well-being. Founded in 1993, Operadora de Fondos de Inversión is one of the most active, fastest growing and expanding companies, with a 16% share in the Mexican financial market.

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

Organizational chart of the Investment Fund Operator



Governance structure

Based on the legal scheme applicable to Principal Grupo Financiero México, Operadora de Fondos de Inversión has a Control Corporate Governance Structure that is responsible for monitoring and supervising the management of investment funds. This structure is made up as follows:

a) Shareholders: With ordinary, extraordinary and extraordinary meetings that are held at least once a year and whose results must be followed by decisions as long as they comply with internal and external regulations.

b) Commissioner; responsible for issuing an annual report on the reasonableness of the financial information presented by the Board of Directors and compliance with internal and external regulations.

c) Board of Directors: composed of at least five members and no more than 15, including responsibilities, but not limited to:

- General Power of Attorney for Acts of Administration.
- To subscribe, accept, issue, endorse and guarantee all kinds of credit instruments on behalf of the Company.
- Opening and canceling bank and investment accounts and/or securities on behalf of the Company.
- To appoint or dismiss the Chief Executive Officer, the External Auditor, the Management and other officers, attorneys-in-fact, agents and employees of the Company.
- Approve the company's financial statements.

d) Investment Meeting: made up of four members of the Risk Management, Investment and Regulatory Controller Departments, with monthly meetings to determine the investment strategy on the securities traded in compliance with the Mexican authority National Banking and Securities Commission (CNBV).

e) Communication and Control Committee: responsible for the prevention and detection of acts, omissions or operations that may promote assistance or cooperation, of any kind, for the commission of the crime related to terrorism or operations with resources of illicit origin.

f) Risk Committee: responsible for identifying, evaluating and managing the risk that could affect the Company's operation.

g) Financial Product Analysis Committee (CRAPF): responsible for establishing and implementing the policies, procedures and guidelines indicated in the Investment Services Circular.

h) Fiduciary Committee: including responsibilities, but not limited to:

- Discuss and approve new trust business.
- To discuss and approve the policies for the adoption, contracting, management and control of all operations derived from fiduciary services.
- Be notified of decisions regarding the results of the periodic evaluation of the customer experience.

i) Chief Executive Officer (CEO): responsible for implementing the business plan, the guidelines of the Board of Directors, the design of the organizational structure, the internal control system, compliance with regulations, as well as leading the development of the Company's operations.

j) Regulatory Controller: responsible for supervising and monitoring the integrity, prestige and quality of the services provided by the Company in compliance with internal and external regulations.

k) Risk Management Manager: define policies, procedures, controls and guidelines for risk management; support 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 on exposure to quantifiable and non-quantifiable risks.

l) Chief Compliance Officer (CCO): including responsibilities, but not limited to:

- Prepare the Compliance Manual.
- To report any conduct, activity or behavior carried out by directors, officers, employees or lawyers, which causes a violation of the Law or the Compliance Manual, in order to impose the corresponding disciplinary measures.

m) Responsible for overseeing compliance with Investment Services.

n) Investment Services Compliance Supervisor in the Advised Investment Services modality: responsible for verifying compliance related to the assessment applied to client profiles and the reasonable analysis of financial products.

o) External Audit.

p) Internal Audit.

Investment Fund Operator Interactions with External Parties

On a daily basis, Operadora de Fondos de Inversión interacts with various external parties in relation to the provision of services to clients. A brief description of the nature of the interaction of these external parties with Operadora de Fondos de Inversión includes:

1. Clients: people involved in the supervision, management or administration of investors. Clients communicate their investment guidelines and objectives to the Investment Fund Operator and are provided with periodic performance reports.

2. Financial Custodians/Administrators: Financial institutions that own the assets and can serve as a ledger (valuation agent) on behalf of clients. Custodians and Financial Managers are hired by the client. The custodian is responsible for the receipt, delivery, and safeguarding of the client's assets. The custodians provide periodic reports to the Investment Fund Operator.

3. Counterparties: refer to the government, national banks, national monetary authorities, and international monetary organizations that act as the final guarantor of loans and indemnities. In addition, the counterparty may refer to brokers, investment banks, and other securities dealers who act as a contracting party when completing "OTC" securities transactions.

4. Pricing and Other Information Providers: Responsible for providing daily and monthly securities prices and corporate action notifications for application to client portfolios. Examples of pricing providers and other information include Integrated Pricing Provider (PiP), Thomson Reuters, Standard and Poor's (S&P), and Bloomberg. Operadora de Fondos de Inversión uses PiP as the primary pricing service, working closely together to help ensure that accurate security prices are received. The Investment Fund Operator may contact PiP in the event that the price of a security does not appear to reflect market activity, providing trading information.

5. Research Providers: Operadora de Fondos de Inversión uses a number of different sources of investment research, including broker and third-party services. While some research may be sources outside the Company, analysts and Portfolio Managers are ultimately responsible for the formulation of strategies and the execution of strategies.

6. Application and Information Technology Consulting Services: Vendors that provide software-as-a-service and back-end support on applications used by the Company.

7. Legal: External firms in legal matters related to investment management and private placement activities.

Compliance and Quality

Operadora de Fondos de Inversión has three quality schemes to support the compliance approach to its operations. First, the main operational areas that seek to improve daily operations; secondly, the Regulatory Comptroller's Office, which provides guidelines on compliance with internal and external regulations; and the Process Improvement Department that helps improve the experience of customers and employees. 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).

Internal Control Overview

An enterprise's internal control is a process, performed by the Board of Directors, management, and other personnel of an entity, designed to provide reasonable assurance with respect to the achievement of objectives related to:

- Reliability of internal and external financial and non-financial information.
- Effectiveness and efficiency of the entity's operations, and.
- Compliance with 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 Integrated Internal Control Framework issued by the Treadway Commission's Committee of Sponsoring Organizations in 2013 for which Investment Fund Operator is using.

Control environment

The control environment is the set of standards, processes, and structures that provide the basis for conducting internal control throughout the organization. It is the foundation of all other components of internal control, providing discipline and structure. The control environment of the Investment Fund Operator is the responsibility of the Chief Executive Officer (CEO), who sets the tone at the top regarding the importance of internal control, including the expected standards of conduct.

The Management of the Investment Fund Operator recognizes its responsibility to establish, communicate and monitor control policies and procedures. Importance is attached to maintaining strong internal control and to the integrity and ethical values of all staff. The resulting control environment has a widespread impact on the overall system of internal control.
Integrity and Ethical Values: The Principal Global Code of Conduct (the Code) serves as the basis for ethical behavior throughout the organization and provides a uniform set of principles for how Board members and employees are responsible for adhering to the Code, conducting business, and performing their duties. The Code is communicated internally via the intranet and is also publicly available on the Company's website. In addition, Principal Grupo Financiero Mexico has an Ethics and Compliance Program, which promotes the core value of Integrity and 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.
- Monitoring the Program.

- Discipline and incentives, and;
- Response and improvement of the Program.

The CCO is responsible for monitoring compliance with the Ethics and Compliance Program together with the Regulatory Controller and Compliance Officers at Principal Grupo Financiero México. Directors and employees are expected to immediately report suspected violations of the Code or laws and suspected unethical or fraudulent activities.

In addition, there are established policies and procedures that cover investment management operations. These policies are high-level statements that set forth the strategic direction, expectations, and scope of various topics and are mandatory for those employees in the stated scope of the policy. 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 to identify, analyze and manage risks to the achievement of its objectives, including the assessment of risks relevant to the preparation of its financial statements and to customers.

Risk Identification and Assessment: The Corporate Risk Department of Principal Grupo Financiero Mexico (PGFM) is responsible for identifying, evaluating and managing risks that may impact the Company's operations or financial information. There is also a Risk Unit that monitors risks related to investment management.
At the corporate level, the risk management model is defined under three lines of defense: the first is made up of the operational areas; they own the risks they identify, evaluate, control and mitigate; its processes are executed in accordance with internal policies and procedures, as well as applicable internal and external regulations, always consistent with the Company's goals and objectives. The second line is responsible for defining policies and procedures that allow for adequate management and control of risks, providing guidelines to the operational areas in order to comply with the above. Finally, the third line is the Corporate Internal Audit Department to provide independent assurance on risk management and internal control carried out by the first and second lines of defense.

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

Control activities

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

The Internal Controls Policy on Financial Reporting and the Supporting Standards require all areas of Principal to maintain certain internal control policies and procedures to help ensure that transactions are properly authorized and accounted for in an accurate and timely manner. They also require that assets are properly safeguarded, that proper segregation of control functions and responsibilities be established and maintained across all functional areas of Principal, and that each area has effective ongoing monitoring procedures in place to ensure that 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 Test Results*.

Information and Communication

Information and communication processes support the identification, capture, and sharing of relevant information from internal and external sources in a form and time frame that enable individuals to fulfill their responsibilities. PGFM has established corporate policies and standards to address reporting requirements, including the identification of data attributes, information repositories, and retention. Information systems consist of procedures, whether automated or manual, for initiating, authorizing, recording, processing, and reporting transactions and maintaining accountability for related assets, liabilities, and actions.
Communication is the continuous, iterative process of obtaining, sharing, and providing necessary information both internally and externally, as appropriate. It includes ensuring that individual roles and responsibilities and information related to internal controls are clearly understood. Communication systems exist from the entity level to the department level. There are multiple avenues of communication to help ensure that processes are working as designed and that issues are identified and resolved in a timely manner. Internal and external reporting and control processes provide sufficient communication of relevant information and the necessary analysis time.

Follow-up activities

Oversight is a critical aspect of internal control to assess whether processes and controls at different levels of the entity are working as intended and whether they are modified as appropriate for changes in conditions. As the first line of defense, operational areas are responsible for the continuous 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, several second-line functions provide continuous monitoring of investment management risks and controls on a regular basis, working closely with line management.

Description of the processing environment

The servers are hosted in two geographically distant data centers interconnected with their own high-speed fiber optics. The production data center is located in Apodaca, Nuevo León and the disaster recovery data center is located in San Pedro Garza García, also in Nuevo León, Mexico. During the period evaluated, one of the applications in the scope was migrated to an AWS cloud data center (primary Virginia and secondary Oregon). The security of these distributed systems is provided by the native security features of the Microsoft Windows operating system, along with application-level security.

Investment Management Systems

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

- Aladdin is an investment software provided by BlackRock to manage the portfolio, understand risk exposure, navigate volatility and the market, and support trading procedures during the period from January 1, 2024, to December 31, 2024. It takes trading and market data, including the buying and selling of securities and derivatives and related accounts receivable and payable. Aladdin creates daily transactions that are used by the investment department and other downstream business processes, such as client reporting.
- SIIF: system used for the determination of the NAV and the generation of mandate statements.
- Solutions: It is the system that manages the accounting of investment funds.

Ivestment Management Processing Services

The following describes the internal controls of Fund Operator that may be relevant to the internal controls of an investment management client. Financial transactions related to customers typically include trading

activity, realized profits and losses, income and expenses, and allocation by sector and shares, and are recorded in various reports/statements provided to customers. A summary of the controls that the investment management client must apply to help ensure that the system operates as intended in its design is provided along with this description. Since computer processing plays an integral role in the overall control environment, the description of the general controls of information systems (see the 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 is a lot of information that needs to be gathered before the account can be invested. This information is set out in the Client's Investment Guidelines charter and must be adhered to by the Investment Manager, as the investment objectives and investment policy to be followed by the client are set out in the aforementioned document.

The Investment Manager is responsible for reviewing the Client's Investment Guidelines letter provided by the client in order to verify whether the desired objectives in terms of returns, risks and assets are achievable and available in the other market; Otherwise, potential changes and feedback are reported to the client according to the desired goals. In addition, the Investment Policy Guidelines will be reviewed by the Investment Department at least once a year, to verify if updates or modifications are required if the client's desired objectives have changed. Once the Investment Guidelines are approved, the Investment Management Agreement (AVI) document is reviewed by the Legal, Compliance and key business leaders involved in the day-to-day operation of the mandate. In the event that no comments or changes arise, it is signed by the client's legal representatives and also by Operadora de Fondos de Inversión.

The investment objectives and restrictions of new clients are clearly documented, communicated and coded within the Aladdin system by the Financial Risk Department to prevent unauthorized transactions. A Customer Profile is created for the dissemination of information to the various employees to maintain and market the customer's portfolio. If changes arise in the client's investment goals and restrictions, these are properly documented and communicated via email to Relationship Management to prevent unauthorized transactions. Next, the Customer Onboarding Department will do the following:

- Send a notification to affected trading partners that the customer profile is available.
- Keep affected trading partners informed of progress, delays, or expected funding dates, and send an email when the account has received funds.
- Coordinate a meeting with all appropriate departments prior to funding.
- Coordinate investment agreements with the Legal Department and all relevant parties.

New Security Configuration and Maintenance

As part of the process of Management of Equity, Fixed Income and Real Estate Portfolios that are listed on the stock exchange, new securities such as Initial Public Offering (IPO) shares, auction of government securities (M Bonds and CETES) or Corporate Securities must be analyzed for purchase. Before a security can be purchased on trading systems, it is recorded in the Securities Master File (SMF). To do this, the Financial Risk Department needs to create a fictitious security in the SMF and review the following, but not limited to, the name of the security, the maturity dates, the security, and, if applicable, the International Securities Identification Number (ISIN). Once the stock market information is available one day after its creation in the SMF, the security will be ready to be traded. The SMF contains qualitative data about each value it has and, also the SMF as part of the Aladdin system, every time an event is updated the information of the values will also be updated in Aladdin for its operation. For values managed through the SIIF system, additions and modifications are made manually.

Access to the SMF is restricted to authorized users within the Financial Risk Department and is also scheduled to restrict the ability to add or change securities to authorized individuals only. Changes must go through

change management processes (IT and/or business approval process), documentation, and submission to the appropriate group prior to migration to a production environment.

Commercial processing

All investment transactions are authorized by the Investment Management of the Investment Fund Operator, as well as reviewed by the corresponding operator or the Portfolio Manager. For each type of account, the Investment Department has authorized certain Portfolio Managers to approve purchases and sales for the applicable Client Accounts. In addition, the Financial Risk Department is responsible for validating that each operation is executed in accordance with the guidelines defined within the Investment Contracts.

For any of the transactions of the Investment Agreement, the Investment 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 Investment Department's trading platforms for execution.

Securities Trading

On a daily basis, the Financial Risk Department is responsible for conducting a review that aims to identify any discrepancies with IMA's guidelines, instructions, and details for any client-directed brokerage arrangement set forth in the Aladdin system by the Investment Department and the actual execution of trades. For this review, a dashboard is in place that shows the tracking of each transaction to verify compliance with the guidelines set forth in one or both of the following schemes: (1) Intraday, in which a warning alert is displayed in case a transaction is not running according to the IMA guidelines before the daily cut-off at 4 p.m. and; (2) Overnight in which a transaction has been executed that is not aligned with the IMA guidelines and this must be notified to the Investment, Compliance and Back Office Departments so that they can take appropriate steps. In both schemes, any inconsistencies or compliance exception alerts are identified, investigated, and resolved in cooperation with the aforementioned departments. On a monthly basis, the Financial Risk Department submits reports on any situation of exception or non-compliance.

Trade Allocation

By aggregating trade orders and assigning the available values, 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 order size. Operadora de Fondos de Inversión adds operations to provide clients with the benefits of efficient and cost-effective delivery of investment management processing services. By adding trades, you can also get more favorable executions and lower broker commissions. Traders have the ability to trade as a block or add orders, based on orders submitted to the desktop and relevant market conditions.

Trades can be done in bulk or in series, where shares are systematically allocated to portfolios on a pro-rata basis where the cost of the shares is averaged to provide clients' portfolios with fair treatment and service. In some cases, a fair and equitable manner may require a non-prorated allowance; Factors such as portfolio guidelines, portfolio composition, tax considerations, and risk tolerance are taken into account when considering a non-prorated allocation.

Best Execution Review

On a weekly basis, the Financial Risk Department reviews a sample of the operations carried out by the Investment Department in order to validate best execution practices. Calls are obtained from the recording system (TEAC in Business-as-Usual situation or AVAYA in case of remote work), Calls are reviewed to validate that the operation has been carried out in accordance with the declarations of the local Investment Manual (Section 2 "Investment Process" – 2.2 "Investment Execution"). Some validated aspects are:

- The existence of at least two citations
- Transactions are executed at the best price and/or market rates
- The time between the quote and the agreement is not more than 30 minutes.

For this review, the Financial Risk Department downloads a report from the Aladdin system with the operations to be validated, with this report they feed the "BEP Monitoring" file which includes historical validations. Subsequently, a sample of calls through the recording system is reviewed, validating the Best Execution practices.

The Financial Risk Department reports monthly to the Investment Department and the Controller of Standards the results of the aforementioned reviews, including observations of operations, issues related to Best Execution (if applicable), as well as opportunities for improvement. If any relevant situation is detected, the Financial Risk Department immediately informs the Investment Department and the Regulatory Comptroller, or the IT Department if it is a problem with the registration system. In addition, the summary of this review is presented quarterly to the Risk Committee.
The Financial Risk Department verifies the functionality of telephone extensions registered with TEAC or AVAYA on a daily basis. Detected issues and/or errors are investigated and resolved. Evidence of this follow-up control is done through an email sent to the IT and Investment team.

Transaction settlement procedures

Before settling the transactions of mandates executed in the Aladdin system, the Custody Department is responsible for confirming that the information of each transaction fixed in the system is aligned with what is indicated in the confirmation letter from the counterparties, which is sent by email to a generic Treasury mailbox. In case differences arise, they are investigated; first from the Investment Fund Operator by the Investment and Custody Departments. It is important to note that the Custody Department reviews the operation by two different users of the department), and then, if applicable, with the Backoffice of the counterparties that will inquire about the root causes of the differences and, where appropriate, send the updated confirmation letter to the aforementioned mailbox. Once the information is accurate, the Department of Custody confirms the agreement in Aladdin. The Aladdin system also has the functionality of generating a letter that confirms the accuracy of the operations; However, this confirmation is only handled internally. In addition, tracking dashboards have been developed to help track process performance.

For those negotiated items related to mandate contracts managed in SIIF, there is an interface of the Aladdin system in which flat files are generated, subsequently imported and reconciled daily with SIIF in order to update the information of the portfolio.

Assessment

Invested shares of clients' accounts are quoted daily. PiP is the provider that Operadora de Fondos de Inversión uses for the valuation of shares. This pricing vector works through an Aladdin system and an interface with it; every night the interface starts working so that the value of all operations recorded in Aladdin is updated.

Annually, the Financial Risk Department conducts tests to verify the accuracy between the prices of Aladdin and PiP, with a margin of variation of +/- 5%. In case of further deviations, these are reviewed in cooperation with PiP and are also discussed during the Risk Committee.

Investment Income and Corporate Actions

Mandatory and voluntary corporate actions, including cash dividends, stock dividends, stock splits, warrants, and margin variance calls, must be notified by the custodian prior to being executed for the knowledge of the local business. In the case of voluntary operations, the Custody Department notifies the Investment Department to carry out an analysis on the different schemes proposed, such as cash or shares, and make the best decision for a better return on investments. It is important to mention that there is a deadline established for the execution of the operation, so in case there is no response from the Investment Department, the operation will be executed under the scheme established by default. Then, once the operation is ready to be executed in the Aladdin system, the Department of Custody will send the response through the corresponding

Custodian system; One authorized user uploads the response, and another approves it to segregation of duties conflicts. There are some cases where the Custodian is notified via email, but this depends on the requirements of each Custodian. In the case of mandatory transactions, the Investment Department will also be notified so that it is aware of and confirms the transaction as mentioned above.

Reconciliations

On a daily basis, the Custodial Secretary performs two reconciliations with the information recorded in the Aladdin system, the 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 the 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 module "Reconciliation Positions-Solutions"; in the event that variations arise, the system will display them through alert notifications so that the Custody Department can proceed with the resolution. For the second, the Custody Department downloads the custody portfolio in an excel file and also generates a report with the information of the Positions in SIIF to reconcile them in Excel, saving the working document and the results. In both cases, if differences arise, they 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 settlements are distributed via email as a farewell.

Customer Reports

Client reports within the scope of this exam are defined within the client's IMA and are generated based on frequency requirements within the IMA.

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

Once the Client's Account Statement is completed, the Financial Risk Department is responsible for sending it to the Customer Service Advisor and then to the client via corporate mail.
The Client Account Statement includes a detailed list of holdings and transactions, portfolio performance and benchmark, characteristics of securities, total market value, and earned income generated by transactions.

It is worth mentioning that there are some customers who do not require a Statement; instead, there are additional reports that must be issued with the frequency and presentation that the client requires through the IMA. In these cases, the Financial Risk Department is not responsible for sending the reports to the client; however, it will review them to ensure that there are no errors before issuing the reports by the Fund Accounting Department.

Privacy Program

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

Previously, the Legal Department strived to strengthen privacy notice practices to preserve the safeguarding of confidential information for all data subjects. In addition, Operadora de Fondos de Inversión has a Data Privacy Office whose objective is to ensure the proper handling of information in compliance with applicable laws, limiting access to data and periodically testing security technology. In the course of business, it is

necessary for Principal Mexico to accumulate, record, store, process, transmit and handle confidential information of customers, employees and the Company. The Company takes these activities very 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 functions. All employees are expected to comply with the Company's privacy and confidentiality practices with respect to 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 the Principal. It is important to mention that the Corporate Privacy Policy, which is available on the Company's internal website for all employees, will be the basis for the development of the aforementioned manual, considering not only the main objective of safeguarding privacy information, but also compliance with the Federal Law on Protection of Personal Data in Possession of Private Parties. LFPDPPP).
Privacy procedures for Principal's processes, including but not limited to the following:

Employees are subject to disciplinary action if they fail to report any breach in accordance with the Corporate Privacy Policy.

Additional information about the Online Privacy Policy can be found at principal.com (https://www.principal.com/privacy-policies).

Business Continuity Program

Operadora de Fondos de Inversión is committed through the Business Continuity Program to protect the financial assets and other interests of its clients. Business continuity works to enable 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 that includes standards, roles and responsibilities and the business continuity plan (BCP). It is published and available to all employees on the Company's intranet. The policy, roles and responsibilities, standards, and plan are reviewed at least once a year or whenever a major amendment occurs. The Business Continuity Program at Principal (Investment Fund Operator) 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 company's business continuity philosophy is to take an all-risk approach, planning for the potential loss of people, facilities, and computer technology, regardless of the cause of the loss. The Company also assumes, for planning purposes, the total loss of the operational site. With plans in place that use this approach and assumption, you can adjust plans to cope with less catastrophic events.

In the event that an incident affects the facility, a company-wide recovery plan is in place for the relocation of business-critical capabilities to an alternate workplace. Business capabilities and processes are considered critical during the first 48 hours of an incident and are identified and prioritized through a formal Business Impact Analysis (BIA) process.
Process owners are responsible for planning the continuity of their operations. The process owners define the business-critical processes, which are then designated to the Financial Risk Department responsible for the development, maintenance, implementation, and execution of the business continuity plan.

Each year, as part of the Business Continuity exercises, each operational area generates a report reporting the results of the tests, as well as identifying actions that may be needed to improve program responses and events. The Financial Risk Department participates as a sponsor of this activity.

In addition, tests are carried out on the Business Continuity Plan, throughout the year, some business continuity exercises are carried out to allow the most effective response during a business interruption. Practicing a recovery team's response helps ensure preparedness in both the solution and personnel during an actual incident. Business continuity exercises are carried out annually and consist of the following:

- Call tree
- Alternative Workplace or Remote Work
- A theoretical exercise with the recovery team of the business area

Additional details of the Business Continuity Program are as follows:

Business Impact Analysis: At least once a year, the Financial Risk Department meets with each process owner to review their processes and risks that may affect the continuity of operations. Each department is ultimately responsible for measuring and managing the risks associated with its business activities. You must understand and take a view of risk across the enterprise, which requires an understanding of the impact your decisions and activities can have on the entire organization. The BIA is held annually at the business area level. The purpose of the BIA is to review the capabilities and processes of the business areas and identify their supporting applications. Based on the Financial Risk of that business area, recovery time objectives are identified for each area capacity and support processes. Helper 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 to when it is resolved. These are usually progressive; however, they can occur simultaneously depending on the nature of the incident. Communication and evaluation will occur throughout the entire lifecycle of an incident. The incident management framework provides processes, tools, and responsibilities 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 impact that the incident may cause.

There are different businesses responsible for incident response within the different levels of the organization such as: Operational Staff, Process Leaders, Department Directors and Local Executive Committee (CEL) Leaders, performing the roles and responsibilities defined in the roles and responsibilities document.

The Investment Fund Operator has established operational response departments to deal with these types of incidents:

- Operative
- THAT
- Cybersecurity
- Privacy
- Site and staff
- Fraud
- Reputation
- Business Continuity and DRP

Each type of incident has its own response criteria depending on its nature and level of severity; However, incident escalation must follow appropriate standards taking into account the estimated impact levels as shown below:

The incident severity levels are 0 – 1 and 2 – 3, with 0 – 1 being the most serious and 2 – 3 being the least serious.

Severity Level 0 – 1: A severe incident is defined as one that significantly affects or stops the flow of operation of Principal (Investment Fund Operator) or that involves a potential severe event that compromises the sensitive information of the client, employee or business and could result in a regulatory, legal or reputational problem. Please note that all severity level 0-1 incidents should be escalated to the Executive Committee leaders involved. In addition, these types of incidents are periodically reported to the Corporate Risk Department by the Financial Risk Department. In the event of an incident of severity level 0-1, BCP's statements and measures, if applicable, will be taken into account.

Severity level 2 – 3: Minor low-impact incident, usually affecting a small portion of customers and may affect with low regulatory and reputational impact. The response to these incidents could be managed by Process Leaders and, if applicable, by Department Directors.

Most escalations begin with operational staff, who must notify their process leader, department director, and in the most severe cases, these must be escalated to the Executive Committee level.

The Investment Fund Operator also has the Incident Management Procedure, which provides guidelines to safeguard the interests of clients and shareholders. The highest level of authority that this procedure has is the Director of Risk and Compliance and it is also approved by the Local Executive Committee.

Disaster Recovery Program

The Disaster Recovery program complements the Business Continuity program, focusing on the recovery of IT systems needed to support business operations and help ensure that recovery plans and exercises position the Company to respond effectively 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 oversees the Disaster Recovery program. The Chief Technology Officer is responsible for helping to ensure the recovery of business area applications and ensuring the recovery of infrastructure systems.

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

Additional details about the Disaster Recovery Program are provided below:

Disaster recovery testing: Critical infrastructure and applications should be tested annually.

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

Information Security Program

A formal Information Security Program has been established to help ensure the protection of the Investment Fund Operator's information assets. At the local level, the Chief Technology Officer and 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 the attention of key events or situations.

There are currently 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 information protection. Annually, the program is submitted to the Chief Technology Officer for approval and to the Information Security Officer to provide guidance on how to configure security components and logical security controls. At the local level, an Information Security Committee is held monthly, in which the main operational areas of the business participate. In addition, on a quarterly basis, the Chief Technology Officer may participate in the Boards of Directors in which he or she presents information security issues and issues.

Likewise, there is a quarterly Compliance report in which key information security metrics and deviations are reported, as well as opportunities for improvement and other concerns for the tools of the servers and workstations so that they can be followed and monitored to improve and strengthen the process. This will help ensure that all departments are committed to monitoring and adhering to this practice.

In addition, there are other reports in which metrics, incidents and information requirements are disclosed in order to take the necessary actions by the assigned managers.

Operadora de Fondos de Inversión understands the importance of privacy and confidentiality of client information. In accordance with applicable laws, a comprehensive written security program is in place that applies to information stored and processed within the Company. High-level components of the program include:

1. Government: which has several principles

    a) Communication and executive support
    b) Information security policies
    c) Collaborators specialized in the field
    d) Information Security Steering Groups

2. Risk management: which has three main initiatives:

a) Security Risk Assessment: There is a process called the IT Risk Project in which the company supports new initiatives or applications that the business requires. Locally, only the routing of requests is addressed and guided.

b) Third-party security profiles: this is a process that consists of evaluating suppliers by carrying out a questionnaire through IRQ (Initial Risk Questionnaire). If any of the four questions get an affirmative answer, the third/external will require a review by the company and then the result is recorded in IT GRC (information security tool). This will make it possible to define action plans and follow up on problems or opportunities for improvement that are identified.

c) Development of a risk assessment framework: in which it is intended that the Financial Risk Department identifies potential risks that may compromise information security in the different operational areas and develops actions to mitigate them.

3. Cyber defense operations and incidents:

a) Threat intelligence: Our corporate has a threat intelligence department that provides a potential threat monitoring service to create awareness and understanding of possible cyber adversaries from different sources. There is a portal that reports cybersecurity news and events to manage these situations.

b) Threat detection and response: There is a Corporate Cyber Defense Department that is responsible for monitoring the network in order to identify and report suspicious activities within the flow of operation of the different departments. If security incidents are identified, the Department of Corporate Cyber Defense will require the assistance of the local Support Center to investigate or format the computer equipment if necessary. In the event that an incident is identified locally, this must be reported immediately to the Corporation.

c) Vulnerability Testing: These tests are performed in 2 ways (1) There is a vulnerability scanning tool managed by the Corporation. At the local level, vulnerability findings are managed by the Systems Infrastructure and Security Departments; however, in case these findings cannot be resolved, these are escalated too Corporate. (2) Penetration tests are conducted annually by a third party in accordance with corporate instructions.

d) Adversary emulation: A dedicated team assesses the ability to defend against cyberattacks in a real-world environment, detect areas of opportunity, and take preventative actions.

e) Incident management and response: There is the ability to detect incidents and carry out the appropriate processes to take prevention and mitigation actions.

f) Preparation exercises: There are preventive exercises simulating real situations, with the intention of allowing the detection of areas for improvement and taking preventive actions to strengthen the incident process.

g) Access identity management. Access identity policies are in place with proper management and directory services. The corporate directory provides the list of active users, as well as the management of the creation or deletion of accounts. Locally, account management activities are limited to locking or unlocking accounts and resetting passwords.

4. Data protection: Operadora de Fondos de Inversión classifies information into four categories: confidential of the client, confidential of the company, internal and public. For all this information management, there are different mechanisms that guarantee the correct use and safeguarding of the information, such as.

    - Data Loss Prevention Program.
    - Tools to monitor all information classified as sensitive (social security numbers, software codes, credit cards, etc.) to prevent information leaks. In case the information is managed outside the organization, it must have the approval of the local management.
    - Managing flash drive devices through port-blocking antivirus and Proofpoint DLP to restrict writing to flash drive devices, and
    - Vulnerability: The GUARDIUM tool scans access to Oracle and SQL databases that deliver reports to database administrators (DBAs) to respond to issues that may arise. Also, corporate reviews through the Active Data Monitoring tool in which any inappropriate situation is reported.

5. Disaster Recovery: Managed through the Business Continuity Program (BCP) and the Disaster Recovery Program (DRP), both aimed at ensuring business continuity by considering operations and systems in the event of a loss event. The BCP is managed by the Financial Risk Department, while the DRP is managed by the Systems Infrastructure Department.

6. Security education and training: Actions are implemented to raise awareness of information security among new and active employees. At the local level, new employees are trained through the Onboarding course, which not only takes into account the general vision of the company, but also the aspects of information security, these actions are recurrent and with updated content

   For active employees, there is also an annual training update on information security topics. In addition, the Investment Fund Operator acá has security courses at least every quarter. In addition, the Department of Local Security sends communications at least once a month.

   In addition, phishing simulations are carried out on all employees, two per quarter, with a total of eight simulations per year. Phishing recognition and reporting skills are put to the test during these simulations. Employees who fail multiple simulations will undergo further training and, depending on the number of simulations failed in a 365-day period, will be subject to consequences according to the number of failures.
   The Information Security Officer aims to provide guidance, training, and support to all employees for the purpose of reminding the Company of best practices, policy updates, and highlighting hot topics related to information security considering the above.

Records Retention Policy

Operadora de Fondos de Inversión retains records of information created for the ordinary course of business for set 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 Record Retention Matrices for each operational area, which are responsible for defining what type of information as well as the retention time should be considered. The matrices include the following, but not limited to type of information, responsible parties, 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 subject of the registration, this period is the minimum time that the Company will retain the registration. The operational area responsible for this record can evaluate the time period to meet the needs of the business. These decisions are also captured in the Records Retention Matrix.

All employees are responsible for properly retaining records, in accordance with this Records Retention Policy, and are required to receive general training in which they obtain instructions on information retention. 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 issues persist, the violation is escalated to compliance.

The administration and safeguarding of the matrices is in charge of the Data Protection Office. Communication of the Policy and review, communication, and verification of the Record Retention Matrices is Compliance; However, maintenance, updates and monitoring are the responsibility of each operational area that will review the matrices annually. Currently, the Compliance Department is strengthening the Records Retention Policy, but any modification issues regarding retention deadlines for each area, it is their own responsibility to keep them up to date. In addition, the Compliance Department, in conjunction with the Corporate, will conduct a review of the Records Retention Policy on an annual basis.

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

In the case of a document hold, the retention rules would be suspended; Records identified as being included in the scope of document retention must be retained until notification is that document retention has been released. This applies to both official copies and duplicates of records.

Information Technology Controls

The following describes Principal's information systems environment, which includes the Investment Fund Operator, 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 procedures of information systems have an impact on the effectiveness of controls in all applications.

System development, maintenance, documentation and change/version control

Principal, through the Configuration Management Policy, guides development staff in designing, testing, and deploying changes to applications and infrastructure. Currently, Operadora de Fondos de Inversión does not carry out any development or design of applications since these are managed through the provider Finanzas y Soluciones, S.C. of the solutions system and the provider Bufete de asesores en sistemas SA de CV de SIIF.

For the purposes of system development, maintenance, documentation, or switching to a new program or to an existing program, a documented business necessity must be submitted (1) by completing certain predefined request forms approved by management, (2) 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 discussing each development, design, or application change with the vendor, a system test is conducted against all programs affected by the requesting user/departmental support group with the assistance of the Information Technology staff. In addition, formal test plans are established to direct the testing effort of the system, as well as a rollback plan in the event of an unforeseen impact on the production environment.

In any of the situations or needs that may arise, either at the request of Operadora de Fondos de Inversión or due to changes required by Finanzas y Soluciones S.C. and Bufete 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 supplier and with any change control management policies or those that apply.

After testing the system, formal approval is obtained from the applicant, tester, and IT head to indicate that the changes have been tested and are ready to be transferred to production. Once the test acceptance approval has been received, the process continues with the next approval step performed by the assigned change and release approvers. Version approvers confirm that all required documents are stored for those involved in the process and are required to retain the information.

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

Documentation: System and program documentation is generated during the various phases of the development/maintenance cycle by development staff. The scope and appropriateness of documentation are the responsibility of the discipline leader, in consultation with the system owner of the department that supports the system. Corporate policy requires that the following be included in each program documentation: (1) documented business need, (2) impact analysis, (3) test plan summary and approval, (4) migration plan, (5) rollback plan, and (6) change and release approvals. This documentation is preserved.

Infrastructure: Due to its nature, most requests for infrastructure changes (e.g., operating systems, utilities, and hardware) may be due to a vendor upgrade, hardware changes, and major changes to system design. Regardless of the nature of the change, the project follows the corporate policy of change control. The Systems Infrastructure Department is responsible for completing most infrastructure changes or those that come from the company.

Change and Release Management: The release and change management processes are designed to (1) help minimize risk to Principal's production environment (IT and technology infrastructure) due to changes, (2) help ensure that changes are made to meet specific business needs, and (3) document accountability and accountability for changes to the environment. To help ensure the stability and high availability of Principal's production environment and technology infrastructure, a formal configuration management policy has been implemented. This policy provides an overall structure while allowing each business unit the flexibility to develop specific procedures for managing changes.

Separate low-environment and production environments are used for distributed applications and management is based on the security features of various access control solutions, some of which are under the control of the vendor.

In the event that emergency changes to the application systems are needed, the appropriate information technology personnel are contacted to correct the problem. In these cases, the authorization procedures are essentially the same as those indicated above; however, they are usually done after the change is implemented. Certain principal and senior-level collaborators have been granted the authority to transfer programs directly from the test and pilot environment to production. All emergency events must follow the change management policy.

Physical access restrictions

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

To access the production data center, there are a few steps that authorized personnel must complete before entering the data center itself. It is important to mention that currently, the only personnel authorized to access the production data center is the Infrastructure Systems Department. First, must be shown to the entrance guard to access the facility's courtyard. Then, the next guard will check the number of the authorized card that each member of the department has and will give the corresponding proximity card to each one. In addition, before accessing the area where the production data center is located, authorized personnel must pass through sensors. The final registration must be made at the reception desk in the area where the production data center is located. There, the receptionist will ask you for basic information, computer recording and also the access number with proximity card, so you get the key to access the final bunker. After that, the proximity card and finally the key will unlock the accesses until entering the production data center. In the event that new access is required, whether temporary or permanent, a form must be submitted to the management of the subcontracted facility and with the corresponding approvals.

As for the Alternate Data Center, access is also controlled by proximity cards that are configured solely for the Department of Infrastructure Systems, as they are the only ones that can access there. In case a third party requires access, you must check in at the reception and at the registry located at the entrance of the data center and a member of the infrastructure department will accompany you permanently throughout your visit. Proximity cards are maintained, managed and controlled by the Access Control area.

With regard to the production data center, even the physical cards are managed by the outsourced administrator, the instructions on who is authorized to access come from the Infrastructure Systems

Department. To access the Alternate Data Center and Treasury Department, proximity cards require additional configuration to access each of these sensitive areas. With regard to the treasury area, the head of this department must notify the Access Control area of any modification that needs to be updated in the configuration of the cards, to ensure the adequacy of the access of authorized personnel. Access to the general areas of the building is also controlled by proximity cards; however, these do not require additional locks.

Proximity cards are issued to all new employees. Additions or deletions in access for all cardholders are formally requested through electronic forms, following all HR steps for hires and terminations in the front office. For the production data center, an electronic form is also sent according to the provider's standards, notifying the corresponding update by persons authorized by the organization for this purpose
Terminated employees must return their access cards to their supervisor after separation, so that the accesses can be removed.

To help ensure that access is appropriate, the Infrastructure Systems Department coordinates and conducts a quarterly review of user access to data centers.

AWS Infrastructure and Triara

The deployment of the Fund Operator's infrastructure is based on the best practices in the industry and has the definition and implementation of robust security policies and procedures that guarantee the existence of controls and monitoring and security mechanisms that allow Control infrastructure to be in a secure environment. The selection of our cloud information hosting service (AWS) providers has the necessary international certifications for the alignment of our definitions.

Consequently, Operadora de Fondos de Inversión has information security policies and procedures, such as physical and logical access controls with the principle of least privilege, authentication processes with the company's Active Directory, two-factor authentication, private connection via the internet, antimalware, firewall, intrusion prevention system, data loss prevention, to mention a few.

Likewise, there are monitoring actions regarding compliance with security controls, both detective and reaction, with scope to perimeter and internal networks.

It is worth mentioning that information security controls are based on NIST standards that allow them to be aligned with best practices, guaranteeing from implementation to monitoring and applicability.

Logical Access Management

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

The Investment Fund Operator uses a documented formal process to grant or revoke access to the Company's resources. System access rights are based on the concept of "need for access to perform business-related operations" and least-privilege access, to help ensure that authorized users have access in accordance with their defined roles or responsibilities.
For Office 365, authentication is provided by Microsoft Authenticator. For the provisioning and deprovisioning of accounts, at the local level, there is a process called ABC (Provisioning, Deprovisioning and Changes) and consists of a request made through a form that is signed by the collaborator authorized for this purpose, to request access when hiring, transferring or firing 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 is sent to the area responsible for the execution of the process. In case the required access rights are different or related to specific topics, the form and information are sent to the Corporate Infrastructure Department for proper treatment. For the deprovisioning in the event of the disincorporation

of collaborators to the company, there is a daily interface with the human resources system in which the access control area detects and executes the corresponding cancellations.

There are monitoring controls such as:

- Monthly Review, consisting of a technical review focused on comparing active collaborators against active users within the scope, with the aim of guaranteeing effectiveness of the execution of cancellations and detecting deviations to take actions.

- Retention of Rights Review (Entitlement Review), consisting of the review by business focused on validating the need for the previously granted access rights, to guarantee the permanence or not of the same and, where appropriate, proceed with the corresponding changes. This review is also carried out for third parties who may have access to the applications or systems. The objective of this "Rights Review" process is to carry out a review of the access rights 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 review and approval. If changes to access rights 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 modification is carried out 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, security for access 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 (e.g., information technology disruptions) and report summary results. This process handles issues that affect a user or a large number of users. When identified, incidents are logged in an incident management tool, and staff monitor open incidents for timely resolution and closure. This is achieved through a Ticket number that will help manage and verify the response given by the Mexico support center. In addition, incidents are assigned a severity level based on the risk and impact they may have. In case the incident is not that serious, the local Support Center will manage and close it, while a serious incident is escalated to the Infrastructure Systems Department to assess the situation and if there is no local solution, the incident will be reported to the headquarters in the United States. With respect to incidents associated with corporate servers, communication equipment, among others, the notification of incidents occurs through a form sent via email to is Tech Ops Operators, (DLISTECHOPSOPERATORS@exchange.principal.com) notifying the event so that they can generate the number of incidents and problems for adequate follow-up.

The main objective of the above is to minimize the impact on business operations that incidents may cause, responding to them as quickly as possible and identifying the root cause to minimize the occurrence.

In addition, the Investment Fund Operator actively monitors the system and information processing to identify any potential incidents.

System Backup: The Investment Fund Operator's policies require that all servers be backed up to provide: (1) processing recovery in the event that data is corrupted or lost, (2) compliance with legal, regulatory, and contractual record-keeping requirements, and (3) data recovery in the event that facilities are lost. This requirement is met through the electronic vault in the data center's virtual tape libraries.

Control Objectives and Related Controls

- CO1 Controls provide reasonable assurance that new accounts and modifications to existing accounts are authorized and configured completely and accurately in accordance with client instructions and guidelines.

1.1 Investment Contracts or mandates signed by both the Authorized Representatives and the client. Aladdin automatically loads the price vector daily and updates all positions within each portfolio.

Note: For 2024 there were no new mandates or investments.

1.2 The investment objectives and restrictions of new clients are clearly documented and codified within the Aladdin system by the Financial Risk Department to prevent unauthorized transactions.

1.3 If changes arise in the client's investment objectives and restrictions (Mandate), these are properly documented and communicated by email to Financial Risk Management to prevent unauthorized transactions. Changes made should be reviewed and approved by the appropriate staff, avoiding segregation of duties (SoD) conflicts.

Note: For 2024 there were no new mandates or investments.

- CO2 Controls provide reasonable assurance that new securities and changes to existing securities are established in the Securities Master File system and reviewed in a complete, accurate, and timely manner.

2.1 Every time there is a new financial instrument on the market, the portfolio manager sends an email to the Financial Risk department, which is responsible for creating and maintaining the databases in the Securities Master File (SMF). Once the financial risk team creates the value in the SMF, they review the critical and manual fields to ensure their accuracy.

Note 1: An email notification will be sent for corporate and private instruments.

Note 2: Government instruments are preloaded directly into the SMF, without the need for email.

Note 3: It is for new instruments in the market, not for Principal, all instruments are already in the SMF

2.2 Dashboards are generated daily to keep track of any identified exceptions and are monitored by the Financial Risk Department.

2.3 The Aladdin system is programmed to restrict the ability to add or change values in the SMF and performance dashboards to only users authorized by the financial risk department.

- CO3 The controls provide reasonable assurance that investment transaction instructions are authorized, executed, and entered into the system in a complete, accurate, and timely manner.

Investment management executes buy or sell orders for approved securities automatically in the Aladdin system whenever required, following pre-configured rules that comply with the established investment regime. This system includes a tool ("Compliance Workbench") to modify investment rules, access to which is restricted exclusively to the Financial Risks area. Modifications are made when changes occur in the portfolio of each investment regime and require the approval of the committees and the regulatory commission before their entry into force.
For client constraints encoded in the 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 before the trade is executed.

In the case of control regime restrictions coded into the Aladdin system, an automated pre-trade/pre-transaction compliance check is executed before execution. Should there be any compliance exceptions, the investment team logs them via the system's dashboard, which then notifies the financial risk team in real-time for tracking and resolution before the operation is executed.

Traders each time they receive trades (simulation with details such as portfolio, amount, side), previously validated by the Portfolio Managers and the financial risk team through the Aladdin dashboard, execute these instructions in the market using the electronic platforms (Bloomberg or MarketAxes) which are programmed to only allow the operation of the instructions.
As a result of this process, an email is generated which contains the key details of the transaction previously validated in Aladdin and at the best level available in the market. Once the transaction is executed, the details of the operation are returned to the system and are recorded again in the Aladdin system.

- CO4 The controls provide reasonable assurance that portfolio guidelines are monitored, and exceptions are identified and resolved in a complete, accurate, and timely manner.

4.2 A warning is issued on Aladdin when compliance issues are identified prior to the negotiation/transaction.

4.3 Compliance exception alerts in Aladdin are identified prior to settlement, tracked, and resolved on the same day by the financial risk team, investments, compliance, and back-office departments. In the event of non-compliance, they are disclosed through a communication with prior approval from the Compliance team and subsequently uploaded to the principal website. Likewise, the non-compliance is registered in the Emisnet system (commission page) so that it can be sent to the investing public and stiv (regulator page).

4.4 On a monthly basis, the Financial Risk Department certifies compliance with clients' investment objectives and restrictions for equity and fixed income accounts.

- CO5 The controls provide reasonable assurance that Management conducts a periodic and systematic review of best execution efforts.

6.1 The Financial Risk Committee is notified quarterly with results and opportunities for improvement related to best execution efforts.

6.3 The Financial Risk Department verifies daily the operation of the extensions registered in the TEAC or AVAYA call tool. Detected discrepancies are investigated and resolved.

6.4 The Financial Risk Department is responsible for reviewing that the best execution process is documented and that backups are in place to ensure continuity of reviews in the event of absence or rotation.

- CO6 The controls provide reasonable assurance that investments are settled, and custodians are informed of transactions in a complete, accurate, and timely manner.

7.1 Each negotiated mandate position, confirmation letters from counterparts are sent to the Custody Team emails and/or the generic Treasury mailbox; therefore, the Department of Custody may conduct a review of the information of the mandates' posts in the Aladdin system and the details in the confirmation letter from the counterparts.

Note: For the period from January 1 to December 31, 2024, there were no mandates.

7.2 Unsettled or failed trades are investigated and resolved by the Custody Department.

- CO7 The controls provide reasonable assurance that investment prices are received from an authorized source and updated in a complete, accurate, and timely manner, and that price cancellations are authorized and processed.

8.4 Aladdin's Financial Risk Department conducts annual reasonableness reviews of prices provided by valuation sources through the ANSER tool. Should exceptions arise, they are investigated and supported. The results are also presented to the Risk Committee. In addition, the automatic valuation is done through an interface between Aladdin and the "PiP" price vector.

- CO8 The controls provide reasonable assurance that investment income, corporate actions, collateral, and margin variation notices are identified and received from an authorized source and updated in the system in a complete, accurate, and timely manner.

9.1 Per event, the Investment Department conducts an analysis for non-government instruments to support best decision-making prior to executing a voluntary corporate action.

Note: Similar analysis is not required for government instruments, as their endorsement by the Federal Government exempts them from this procedure.

9.2 For voluntary actions, confirmations are made through the Custodian's system or by email. For confirmations through the system, one authorized user uploads the response and another approves it.

- CO9 The controls provide reasonable assurance that security positions and cash balances reflected in investment management systems are reconciled completely, accurately, and timely with actual positions and balances.

10.1 The custodian team automatically generates a reconciliation between the Aladdin system and Portfolio Net on a daily basis in the "Reconciliation of Positions-Solutions" module. In case any discrepancy is identified, it is investigated and resolved by the Custody Department.

- CO10 The controls provide reasonable assurance that client reports and billing are accurate, complete, and provided to clients in a timely manner.

11.1 The financial risk team generates monthly reports for mandate clients from the Aladdin system. Validation is performed by the Operations Team in conjunction with the Custody and Accounting Teams.

11.2 The Customer Service Advisor distributes the reports to customers at least once a month via email, if any problems are identified, corrections are made prior to the delivery of the report in the Aladdin system.

11.3 Before terminating or interrupting the contract earlier than agreed, final fee invoices are generated and prorated by the Financial Risk Team until the termination date.

Note: For the period to be evaluated from January 1 to December 31, 2024, there were no terminations of mandate contracts

- CO11 The controls provide reasonable assurance that:

Application code changes and configuration parameters are initiated as needed, authorized, and operate according to application specifications to (1) produce valid, complete, accurate, and timely processing and data, (2) ensure application control functionality, and (3) support segregation of duties.

The network infrastructure is configured as authorized to (1) enable applications and application controls to operate effectively, protect data from unauthorized changes, (3) provide availability for processing, and (4) support segregation of duties.

12.1 The primary change control policy is used to guide development staff in designing, testing, and deploying changes to infrastructure and applications.

12.2 Eventually, the application form is submitted by the application stakeholder and approved by the appropriate Department Leader to develop a new program or change an existing program.

Note: The Head Office manages the administrator users of the change tool.

12.3 System testing is performed on all programs affected by the requesting departmental or user support group with the assistance of information technology staff in a test environment. Formal test plans are developed to direct the testing effort of the system.

12.4 Controls associated with the system's change management process: (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 version approver is restricted to selected personnel. This access is provided by Business Unit contacts with management approval.

12.5 After system testing, formal approval is obtained from the requester/tester of the requesting user and/or the support group staff involved in the testing to indicate that the changes have been tested and are ready to be transferred to production. Once the test acceptance approval has been received, the change continues to the next approval step, which is performed by the assigned change and version approvers. Version approvers confirm via email that all required documents are stored for those involved in the process and are required to retain the information. Emergency changes will be managed and documented in accordance with the statements in the Change Control Policy.

12.6 All required changes or needs to the system are monitored quarterly by stakeholders, and these changes are selected from a sample of the transfer history report to validate the following: (1) each change was appropriate, (2) documentation was retained, and (3) necessary approvals were obtained.

12.7 Environments, database development and SIIF application and Solutions

The Development area requests the restoration of the development environments of the databases and applications to the infrastructure team by email whenever required. This application requires pre-approval from the Technical Development Leader and the Infrastructure area. Infrastructure then performs the restore by obfuscating the data in accordance with the Data Obfuscation Procedure in the case of SIIF and confirms the completion of the request execution via email or Teams.

Note: For development environments in the SIIF and Solutions applications, developers have written and read permissions.

12.7.1 Test environments, databases and SIIF application and Solutions

The Development area requests the restoration of the test environments of the databases and applications to the infrastructure team by email whenever required, so that later environment can be used to perform tests with end users. This application requires pre-approval from the Technical Development Leader and the Infrastructure area. Subsequently, Infrastructure performs the restoration of the test environments and confirms the completion of the execution of the request by email or Teams.

Note: For test environments in the SIIF and Solutions applications, developers and end users have written and read permissions.

12.7.2 Production environments, databases and SIIF application

The infrastructure area, at the request of the development team, prepares the production environment. The changes controls that affect the production environments are executed in accordance with the Change Control Policy and Procedure, whose management mechanism of the service lifecycle of the Jira tool.

- CO12 The controls provide reasonable assurance that physical access to data centers and other sensitive areas is restricted to authorized and appropriate personnel.

13.1 Access is restricted to the facilities of Principal Fondos de Inversión, S.A. de C.V. Operadora de Fondos de Inversión at the entrances of the buildings and at the doors of sensitive areas within the buildings (e.g., computer rooms) using electromechanical locks controlled by proximity card, with additional configuration for sensitive areas. In the event of a safety device failure, documented mitigation processes are in place.

Note: Principal Inversiones' offices are classified by location and sensitive areas:

- In Monterrey (Corporativo Valle) are the sensitive areas of Custody, IT, Accounting and Commercial.
- The sensitive areas of Financial Risk, Investments and General Management are located in Mexico City (Corporativo Carso).

13.2 The Infrastructure Systems team conducts a semi-annual email review of users who are granted access to the data centers.

13.3 Physical accesses are removed when a user is unsubscribed. A notification is made to the Infrastructure System team to proceed with the update in the proximity card system to disable the cards of terminated employees.

- CO13 The 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 modifications and support segregation of duties.

14.1 Policies, standards, and procedures are set in all major information resources to set requirements for how to configure security components and logical security controls.

14.2 For account provisioning and deprovisioning, the ABC process is carried out when the requesting user submits a request form approved by the Department Head to the Support Center that validates that the access request is appropriate according to the job functions. In the event that specific access rights are needed, the Support Center notifies the Corporate Infrastructure Team for appropriate treatment.

Note 1: Approval for the provisioning of accounts is made by the Head of Department, based on his or her criteria of expertise.

Note 2: For Solutions, the provisioning and deprovisioning flow applies to the application, not to the databases. This is because "Database as Filesystem" (DBaaS) is used, which allows access to the file system interface to users in the support and treasury center.

14.3 A monthly technical review is conducted to identify employee terminations to disable accounts or access rights in applications and/or systems (SIIF, Solutions, Aladdin). Third parties granted access rights are also considered within the review.

14.4 Accounts with no registration activity for a period longer than 90 days are automatically blocked or disabled.

14.5 User access review is conducted at least annually by the IT Department in conjunction with process owners for access rights granted to critical applications. If discrepancies are identified, they are evaluated to define whether or not access should remain.

Note: For the Aladdin application, the review is done semi-annually through mail.

14.6 Windows security settings are reviewed quarterly by Information Security and Risk. Configurations that do not meet defined security standards are reported to the CIO Working Group

- CO14 The controls provide reasonable assurance that application and system processing is authorized and executed completely, accurately, and timely; and that deviations, issues, and errors are identified, tracked, recorded, and resolved completely, accurately, and timely. The controls provide reasonable assurance that data and application backups are made to allow restoration of applications and processing in case of data or application destruction.

15.1 Principal Fondos de Inversión, S.A. de C.V. Operadora de Fondos de Inversión actively monitors networks, services, operating systems and databases in the system and information processing to identify incidents. When identifying incidents, the user is responsible for reporting the incident to the Support Center, which generates the ticket and assigns it to the appropriate level based on severity for a timely response.

15.2 Servers are backed up daily and replicated to the disaster recovery data center.

Note 1: By November 15 and 16, 2024, the Backup process changed to AWS.
Note 2: For the period to be evaluated, no backup restores were requested for the SIIF and Solutions applications.

15.3 When registering and coding new Counterparties in Aladdin, these must be approved by the Risk Committee. In addition, the Financial Risk Department conducts a review on a quarterly basis to confirm accuracy between counterparties on the Approved Counterparties List and the Aladdin system. Any concerns or discrepancies identified are investigated and resolved.

15.4 A daily reconciliation is made between PortafoliosNet and the portfolio provided by the custodian, positions are composed as cash. In case any discrepancies are identified, they are investigated and resolved by the Custody Department. Conciliations are recorded through a .xls and the Custodian team reviews and approves the reconciliations (signed or electronically or by email).

15.5 The configuration of the jobs is executed from the change management process through the Jira tool, in the release format the script to be executed is described to be tested in the development and test environments, and then the infrastructure team implements in the SIIF production environment through SQL Server.

Note 1: On November 15 and 16, 2024, the migration to AWS infrastructure for the SIIF application was carried out and all jobs were reconfigured.

Note 2: For Solutions there are no jobs, Database as Filesystem is used.

CO14 The controls provide reasonable assurance that block orders are allocated to customers in a fair manner.

16.1 At least once a year, the Investment Department qualitatively and quantitatively assesses the service levels provided by counterparties throughout the terms of the mandates to review the fairness of the allocation process.

16.2 The Financial Risk area, in conjunction with the investment area, reviews daily that the investment portfolio complies with the investment regime, the deviations detected that break the regime of the assignment procedures through the Aladdin dashboards, are escalated to the Compliance

Department, investigates and resolves the identified exceptions.

16.3 A strategy meeting is held monthly with the investment team, risks, the CEO, the leaders of each area (if applicable), as a result of this process the Investment team communicates the strategy through a presentation with the trading and the investment portfolio on the positions of the mandates attending the monthly meeting of the Committee, the follow-up of which is agreed at the session.

Complementary Controls of User Entities (CUEC'S)

Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos de Inversión, Principal Grupo Financiero, declares that there are no complementary controls of the user entities detected in the management system associated with Investment Management System, supported by Aladdin, SIIF and Solutions used for the registration and monitoring of investments.), so no additional controls that user organizations must have to complement the Investment Management Processing Services and Information Technology controls are described.

Relevant Aspects of the Control Environment, Risk Assessment, Monitoring of the Components of the Internal Control of Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos de Inversión, Principal Grupo Financiero

No changes were made to the internal control system for the evaluation period from January 1, 2024, to December 31, 2024.

SECTION IV

Description of the Design Suitability and Operational Effectiveness of controls

Description on the Suitability of Design and Operational Effectiveness of Controls at Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos de Inversión, Principal Grupo Financiero

This report presents the results of control testing performed by the Service Auditor, in relation to the objectives and controls defined by Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos de Inversión, Principal Grupo Financiero. To evaluate the control environment, management criteria established in the Internal Control System were considered. These same criteria guided the design, implementation, and evaluation of the effectiveness of the tests applied to the specific controls, detailed in Section IV. Additionally, observation and inspection procedures were used to evaluate the completeness and accuracy of information on reports, queries, listings, documents, and relevant system records, to verify the completeness and accuracy of the information used as evidence in the testing of control activities.

Information Produced by the Entity (IPE)

When planning the nature, timing, and extent of our testing of controls specified by Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos de Inversión, Principal Grupo Financiero, the control environment, risk assessment processes, information and communication, and management monitoring procedures, we considered the testing procedures as follows:

Procedures for evaluating the completeness and accuracy of Information Produced by the Entity (IPE): For testing controls that require the use of IPE, procedures were performed to evaluate the reliability of the information, including the 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 original documentation related to the IPE.
- Inspection of the query, script, or parameters used to generate the IPE.
- Data agreed between the IPE and the source.
- Inspection of management procedures.

Control objectives 1
The controls provide reasonable assurance that new accounts and modifications to existing accounts are authorized and modifications to existing accounts are authorized and configured according to customer and guidelines of the customer in a complete and accurate manner accurate.

Control Id	Description of Principal's control	Procedure developed by EY	Test Result
1.1	Investment Contracts or mandates signed by both the Authorized Representatives and the client. Aladdin automatically loads the price vector daily and updates all positions within each portfolio. Note: For 2024 there were no new mandates or investments.	Inquired about the process for investment contracts or mandates. It was indicated that investment contracts or mandates must be signed by both the authorized representatives and the client. Once signed, the Aladdin tool automatically loads the price vector daily and updates all positions within each portfolio. We were informed that there were no new mandates or investments for the year 2024. The record of new mandates or investments in the Aladdin system for the evaluated period was requested and reviewed. Observed the data generation from the Aladdin system. It was confirmed that no new mandate contracts or investments were registered during the year 2024.	No new investment contracts or mandates were created during the reporting period, confirmed by inquiry with the Risk Manager and inspection of the output from the Aladdin system-generated Aladdin.
1.2	The investment objectives and restrictions of new clients are clearly documented and codified within the Aladdin system by the Financial Risk Department to prevent unauthorized transactions.	Inquired about the process for documenting and codifying new clients' investment objectives and restrictions within the Aladdin system. It was indicated that the Financial Risk Department is responsible for ensuring these are clearly and accurately recorded to prevent unauthorized transactions. Inspected the Financial Risk Department's internal documentation related to the codification process in Aladdin, including applicable policies and procedures. Given the confirmation that no new mandates or	No exceptions No exceptions

Control Id	Description of Principal's control	Procedure developed by EY	Test Result
		investments were registered in 2024, the inspection focused on the existence and updates of the codification procedures. Observed the data generation from the Aladdin system on April 4, 2025. It was confirmed that no new mandate contracts or investments were registered during the year 2024, meaning no new investment objectives or restrictions were processed in the audited period. Observed the coding of Constraints Rules for existing mandates and validated the coded investment constraints directly in the Aladdin system.	No exceptions No exceptions
1.3	If changes arise in the client's investment objectives and restrictions (Mandate), these are properly documented and communicated by email to Financial Risk Management to prevent unauthorized transactions. Changes made should be reviewed and approved by the appropriate staff, avoiding segregation of duties (SoD) conflicts. Note: For 2024 there were no new mandates or investments.	Inquired about the process for modifying existing clients' investment objectives and restrictions (mandates). It was indicated that any changes to mandates must be properly documented and communicated via email to Financial Risk Management to prevent unauthorized transactions. Furthermore, we were informed that changes made should be reviewed and approved by appropriate staff, avoiding segregation of duties (SoD) conflicts. Inspected the documentation of internal policies and procedures of the Financial Risk Management area related to managing changes in investment mandates. Given that there were no new mandates or investments for the year 2024, the inspection focused on the existence and adequacy of such procedures for handling potential future modifications.	No new investment contracts or mandates were created during the reporting period, confirmed by inquiry with the Risk Manager and inspection of the output from the Aladdin system-generated Aladdin.

Control objectives 2
Controls provide reasonable assurance that new securities and changes to existing securities are established in the Securities Master File system and reviewed in a complete, accurate, and timely manner.

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
2,1	Every time there is a new financial instrument on the market, the portfolio manager sends an email to the Financial Risk department, which is responsible for creating and maintaining the databases in the Securities Master File (SMF). Once the financial risk team creates the value in the SMF, they review the critical and manual fields to ensure their accuracy. Note 1: An email notification will be sent for corporate and private instruments. Note 2: Government instruments are preloaded directly into the SMF, without the need for email. Note 3: It is for new instruments in the market, not for Principal, all instruments are already in the SMF	Inquired about the process for creating and maintaining the database in the *Securities Master File* (SMF) for new financial instruments in the market. Informed that for corporate and private instruments, the portfolio manager sends an email to the Financial Risk department. This department is responsible for creating the instrument's value in the SMF and reviewing critical and manual fields to ensure their accuracy. It was clarified that government instruments are preloaded directly into the SMF, without the need for email notification. It was also emphasized that this process applies only to new instruments in the market, not to those already existing in the main portfolio. Inspected the Financial Risk department's policy and procedures related to the creation and maintenance of new instruments in the SMF. We reviewed evidence of email communication from the portfolio manager for corporate and private instruments, as well as records of the creation and review of values in the SMF. For government instruments, we examined records of their direct preloading.	No exceptions No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
		Observed the process of creating a new financial instrument (corporate or private) in the SMF, from receiving the email from the portfolio manager to the Financial Risk team's review of critical and manual fields. For government instruments, we observed the SMF interface to verify automatic preloading and data integrity.	No exceptions
2,2	Dashboards are generated daily to keep track of any identified exceptions and are monitored by the Financial Risk Department.	Inquired about the process for generating and monitoring dashboards that track identified exceptions. It was explained that these dashboards are generated daily and are monitored by the Financial Risk Department. Inspected the Financial Risk Department's procedural documentation related to the generation and use of exception dashboards. Evidence of the daily generation of these dashboards and records of actions taken in response to identified exceptions, such as reviews performed by responsible personnel, were examined. Observed the real-time dashboard interface, verifying its daily updates and how the Financial Risk Department uses it to identify and manage exceptions. The system's ability to present clear and timely information on any deviations or anomalies was validated.	No exceptions No exceptions No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
2,3	The Aladdin system is programmed to restrict the ability to add or change values in the SMF and performance dashboards to only users authorized by the financial risk department.	Inquired about how the Aladdin system restricts the ability to add or change values in the Securities Master File (SMF) and performance dashboards. It was explained that the system is programmed to allow these actions only to users who have been specifically authorized by the Financial Risk Department.	No exceptions
		Inspected the security configuration and user profile logs in the Aladdin system. It was verified that permissions to add or modify values in the SMF and on performance dashboards are exclusively assigned to users designated by the Financial Risk Department. Additionally, the internal procedures of department for access management and role assignment were reviewed.	No exceptions
		Observed a live demonstration of the access restriction functionality in Aladdin. An attempt was made, with an unauthorized user, to add or change a value in the SMF and on the performance dashboards, confirming that the system prevented the action. Subsequently, an authorized user was observed successfully performing these operations, validating the effectiveness of the control.	No exceptions

Control objectives 3
The controls provide reasonable assurance that investment transaction instructions are authorized, executed, and entered into the system in a complete, accurate, and timely manner.

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
3,1	Investment management executes buy or sell orders for approved securities automatically in the Aladdin system whenever required, following pre-configured rules that comply with the established investment regime. This system includes a tool ("Compliance Workbench") to modify investment rules, access to which is restricted exclusively to the Financial Risks area. Modifications are made when changes occur in the portfolio of each investment regime and require the approval of the committees and the regulatory commission before their entry into force.	Inquired about how the Aladdin system automatically executes buy or sell orders for approved securities and how it ensures compliance with pre-configured investment rules. We were informed that the system includes a tool called "Compliance Workbench" to modify these rules, and that access to this tool is restricted exclusively to the Financial Risk department. Modifications are made when changes occur in the portfolio of each investment regime and require the approval of relevant committees and the regulatory commission before they become effective.	No exceptions
		Inspected the Aladdin system's configuration for pre-configured investment rules and the access logs for the "Compliance Workbench" tool, verifying that only authorized personnel from the Financial Risk department have modification permissions. The internal procedures for rule modification were reviewed, including evidence of the required approvals from committees and the regulatory commission before any changes were implemented.	No exceptions
		Observed a live demonstration of an automatic buy or sell order execution in the Aladdin system, validating that the system only allows transactions that comply with the established investment rules. Additionally, the process of modifying a rule in the "Compliance Workbench" by an authorized user was observed, confirming access controls and approval workflows.	No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
3,2	For client constraints encoded in the 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 before the trade is executed.	Inquired about the process for automatic pre-trade compliance checks within the Aladdin system. We were informed that for client constraints encoded in the 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 before the trade is executed. Inspected the Aladdin system's configuration for pre-trade compliance rules and the logs of generated exceptions. We reviewed evidence of how the system identifies real-time deviations from client restrictions and how these are tracked until their resolution, to ensure that no transaction is executed without complying with the established parameters. Observed a live demonstration of a transaction that generated a pre-trade compliance exception in Aladdin. We verified how the system halts trade execution, how the exception is notified, and how its resolution is managed before allowing the transaction to proceed.	No exceptions No exceptions No exceptions
3,3	In the case of control regime restrictions coded into the Aladdin system, an automated pre-trade/pre-transaction compliance check is executed before execution. Should there be any compliance exceptions, the investment team logs them via the system's dashboard, which then notifies the financial risk team in real-time for tracking and resolution before the operation is executed.	Inquired about the automated pre-trade/pre-transaction compliance check within the Aladdin system, specifically how it handles control regime restrictions. We learned that the system automatically performs this check before any transaction is executed. Should a compliance exception arise, the investment team logs it via the system's dashboard.	No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
		This action triggers a real-time notification to the financial risk team for immediate tracking and resolution, ensuring the operation isn't executed until the issue is resolved.	No exceptions
		Inspected the system's configuration of pre-trade compliance rules for regime restrictions and reviewed logs of generated exceptions. Our focus was on confirming that the system correctly identifies deviations from defined regime constraints and that the logging and real-time notification mechanisms to the financial risk team function as described. This helps ensure that no operation proceeds if it violates the established regime.	No exceptions
		Observed a live demonstration of a transaction that triggered a regime compliance exception in Aladdin. We verified how the system halts execution, how the investment team logs the exception on the dashboard, the real-time alert to the financial risk team, and the subsequent resolution process that must occur before the transaction is allowed to continue.	No exceptions
3,5	Traders each time they receive trades (simulation with details such as portfolio, amount, side), previously validated by the Portfolio Managers and the financial risk team through the Aladdin dashboard, execute these instructions in the market using the electronic platforms (Bloomberg or MarketAxes) which are programmed to only allow the operation of the instructions.	Inquired about the IT/DT (Information Technology/Data Transaction) process for how traders execute orders in the market and how data flows through the systems. We learned that traders receive trading instructions that have been previously validated by Portfolio Managers and the financial risk team via the Aladdin dashboard. These instructions are executed in the market using electronic platforms (Bloomberg or MarketAxes) which are programmed to only allow the operation of validated instructions.	No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
	As a result of this process, an email is generated which contains the key details of the transaction previously validated in Aladdin and at the best level available in the market. Once the transaction is executed, the details of the operation are returned to the system and are recorded again in the Aladdin system.	As a result of the execution, an email is generated containing the key details of the transaction (already validated in Aladdin and at the best market level). Once the transaction is executed, the details of the operation are returned to the system and automatically recorded in Aladdin. Inspected the configuration and audit logs of the electronic platforms (Bloomberg/MarketAxes) to confirm that they only allow the execution of previously validated instructions. We reviewed the traceability records of trades from the Aladdin dashboard to the execution platforms and back to the system. This included verifying the data integrity in the generated emails and their correspondence with the final records in Aladdin. Observed an end-to-end simulation of a trading cycle in the production environment (or a replicated test environment). This allowed us to verify the automation of initial validation in Aladdin, the restriction of electronic platforms to authorized instructions, the automatic generation of the email as an execution record, and the automatic return and recording of transaction data in Aladdin, confirming the integrity and fluidity of the IT/DT process.	No exceptions No exceptions No exceptions

Control objectives 4
The controls provide reasonable assurance that portfolio guidelines are monitored, and exceptions are identified and resolved in a complete, accurate, and timely manner.

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
4,2	A warning is issued on Aladdin when compliance issues are identified prior to the negotiation/transaction.	Inquired about the process by which the Aladdin system issues warnings when compliance issues are identified prior to negotiation or transaction. We were informed that the system is programmed to automatically generate and display a real-time warning when a potential breach of compliance rules is detected before an operation is executed.	No exceptions
		Inspected the configuration of pre-trade compliance rules within the Aladdin system and the parameters that trigger the issuance of these warnings. System logs were reviewed to identify instances where warnings were generated due to compliance issues, and it was verified that the warning prevented the transaction from being executed until the issue was addressed or resolved.	No exceptions
		Observed a live demonstration of a transaction that intentionally violated a pre-trade compliance rule. It was verified that the Aladdin system issued the expected warning, halted the transaction's progression, and not allow its execution until the compliance condition was resolved or overridden by authorized personnel (if applicable and under defined procedures).	No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
4,3	Compliance exception alerts in Aladdin are identified prior to settlement, tracked, and resolved on the same day by the financial risk team, investments, compliance, and back-office departments. In the event of non-compliance, they are disclosed through a communication with prior approval from the Compliance team and subsequently uploaded to the principal website. Likewise, the non-compliance is registered in the Emisnet system (commission page) so that it can be sent to the investing public and stiv (regulator page).	Inquired about the process for validating and resolving compliance exception alerts in Aladdin. The risk team confirmed that this validation is performed prior to settlement. We were informed that non-compliance communications, once approved by the Compliance team, are uploaded to the main website and sent to the regulator's page, serving as key supporting documents. Inspected publications on the main website as well as evidence of referrals to the regulator for 2024. It was verified that these communications contained the expected fields: Regime, Limit, and Observed Position. Observed that the results of the non-compliance validation provided reasonable assurance that portfolio guidelines are monitored and that exceptions are identified and resolved in a complete, accurate, and timely manner.	No exceptions No exceptions No exceptions
4,4	On a monthly basis, the Financial Risk Department certifies compliance with clients' investment objectives and restrictions for equity and fixed income accounts.	Inquired with the risk team the certification of compliance if the validation of clients' investment objectives and restrictions is carried out for variable income and fixed income accounts monthly this occurs and confirmed the power point presentation remains as a supporting document. Inspect the power point for 2024 which contains the following fields: - Portfolio position - Portfolio returns - Investment regime	No exceptions No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
		Observed that, as a result of the validation, it was determined that provide reasonable assurance that portfolio guidelines are monitored and exceptions are identified and resolved completely, accurately, and in a timely manner.	No exceptions

Control objectives 5
The controls provide reasonable assurance that Management conducts a periodic and systematic review of best execution efforts.

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
6,1	The Financial Risk Committee is notified quarterly with results and opportunities for improvement related to best execution efforts	Inquired about the process of notifying the Financial Risk Committee regarding best execution efforts. We were informed that this committee is notified quarterly with results and identified opportunities for improvement in this area. Inspected the minutes or presentations from the Financial Risk Committee meetings for the quarters corresponding to the evaluated period. It was verified that these minutes included the results of best execution efforts and, where applicable, identified opportunities for improvement, as well as evidence of review and discussion by the committee members.	No exceptions No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
		Observed through reviewing recordings or participating in a session the presentation of best execution results and improvement opportunities to the Financial Risk Committee, confirming the quarterly frequency of this notification and the attention given to it within the committee's agenda.	No exceptions
6,3	The Financial Risk Department verifies daily the operation of the extensions registered in the TEAC or AVAYA call tool. Detected discrepancies are investigated and resolved.	Inquired with the Financial Risk team Checks the operation of the extensions registered in the TEAC or AVAYA call tool daily and confirmed the supporting screens validated from tool remains as a supporting document. Inspect the screens from tool for 2024 which contains the following fields: - Call start - Duration - Service - Skill - Call ID Observed that, as a result of call monitoring at the tool, it was determined that the Administration conducts a periodic and systematic review of the best implementation efforts.	No exceptions No exceptions No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
6,4	The Financial Risk Department is responsible for reviewing that the best execution process is documented and that backups are in place to ensure continuity of reviews in the event of absence or rotation.	Inquired with the Financial Risk Department about its responsibility to ensure the best execution process is documented and that backups are in place to ensure the continuity of reviews in the event of absence or rotation. We were informed that any manual updates are performed manually and do not involve extracting data from computer equipment.	No exceptions
		Inspected the documentation of the best execution process to verify its existence and that of backup plans to ensure the continuity of reviews. Given the information that no manual revisions were submitted in 2024, our inspection focused on the existence and adequacy of the policy and procedures that establish this responsibility for the Financial Risk Department.	No exceptions
		Observed through an interview or review of procedures the Financial Risk Department's approach to documenting the best execution process and maintaining the necessary backups. We confirmed that, although there were no updates in 2024, the process for handling them in the future is established.	No exceptions

Control objectives 6
The controls provide reasonable assurance that investments are settled, and custodians are informed of transactions in a complete, accurate, and timely manner.

Control ID	Description of Principal's control	Procedure developed by EY	
7,1	Each negotiated mandate position, confirmation letters from counterparts are sent to the Custody Team emails and/or the generic Treasury mailbox; therefore, the Department of Custody may conduct a review of the information of the mandates' posts in the Aladdin system and the details in the confirmation letter from the counterparts. Note: For the period from January 1 to December 31, 2024, there were no mandates.	Inquired about the process for verifying negotiated mandate positions against counterparty confirmations. We were informed that confirmation letters from counterparts for each negotiated mandate position are sent to the Custody Team's emails and/or the generic Treasury mailbox. This allows the Custody Department to review the mandate positions' information in the Aladdin system and compare it with the details in the counterparty confirmation letter. Inspected the evidence of communications (emails) sent to the Custody Team and/or the Treasury mailbox. Given the that for the period from January 1 to December 31, 2024, there were no new mandates, our inspection focused on the existence and adequacy of the Custody Department's procedures for conducting this information review. Observed (by reviewing documented procedures or conducting an interview) how the Custody Department would perform the review of mandate position information in Aladdin against counterparty confirmation letters, confirming that the process is established, even though it was not activated in 2024 due to the lack of new mandates.	No new investment contracts or mandates were created during the reporting period, confirmed by inquiry with the Risk Manager and inspection of the output from the Aladdin system-generated Aladdin.

Control ID	Description of Principal's control	Procedure developed by EY	
7,2	Unsettled or failed trades are investigated and resolved by the Custody Department.	Inquired about the process by which the Custody Department investigates, and resolves unsettled or failed trades. We were informed that this department is responsible for taking action when a transaction does not settle correctly or fails.	No exceptions
		Inspected the records of unsettled or failed trades for the evaluated period. Documented cases where the Custody Department intervened were reviewed, verifying evidence of the investigation conducted and the actions taken to resolve the situation. Follow-up reports and internal or external communication related to these events were examined.	No exceptions
		Observed through reviewing documented cases or a simulation of the process how the Custody Department addresses an unsettled or failed trade. The process of identifying the issue, assigning responsibilities for the investigation, communicating with involved parties, and the steps followed until the final resolution of the trade were verified.	No exceptions

Control objectives 7
The controls provide reasonable assurance that investment prices are received from an authorized source and updated in a complete, accurate, and timely manner, and that price cancellations are authorized and processed.

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
8,4	Aladdin's Financial Risk Department conducts annual reasonableness reviews of prices provided by valuation sources through the ANSER tool. Should exceptions arise, they are investigated and supported. The results are also presented to the Risk Committee. In addition, the automatic valuation is done through an interface between Aladdin and the "PiP" price vector.	Inquired with the Financial Risk Department about their process for conducting annual reasonableness reviews of prices provided by valuation sources. We were informed that this review is performed using the ANSER tool. Should exceptions arise, they are investigated and duly supported. The results of these reviews are also presented to the Risk Committee. Additionally, it was explained that automated valuation is carried out through an interface between Aladdin and the "PiP" price vector, ensuring continuous updates of values.	No exceptions
		Inspected the Financial Risk Department's procedural documentation for the annual price reasonableness review using the ANSER tool, including criteria for identifying and supporting exceptions. We reviewed the reports and presentations submitted to the Risk Committee detailing the results of these annual reviews. For automated valuation, we examined the documentation of the interface between Aladdin and the PiP price vector, as well as logs of the interface's execution to confirm its operation.	No exceptions
		Observed through a demonstration the functionality of the ANSER tool for price reasonableness review and the process for investigating and supporting exceptions. The presentation of results to the Risk Committee was validated.	No exceptions
		Observed that the operation of the interface between Aladdin and the PiP price vector was observed, confirming that automated valuation is performed continuously and accurately.	No exceptions

Control objectives 8
The controls provide reasonable assurance that investment income, corporate actions, collateral, and margin variation notices are identified and received from an authorized source and updated in the system in a complete, accurate, and timely manner.

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
9,1	Per event, the Investment Department conducts an analysis for non-government instruments to support best decision-making prior to executing a voluntary corporate action. Note: Similar analysis is not required for government instruments, as their endorsement by the Federal Government exempts them from this procedure.	Inquired with the investment team about the analysis performed for non-governmental instruments prior to executing a voluntary corporate action. We were informed that this analysis is conducted on a per-event basis to support optimal decision-making, and that prepared presentations serve as key supporting documentation. It was clarified that a similar analysis is not required for governmental instruments, as their endorsement by the Federal Government exempts them from this procedure. Inspected the quantitative and qualitative monitoring and analysis performed to support improved decision-making. We reviewed the presentations documenting these analyses, verifying their content and the depth of the support provided. Given the "per-event" nature of this control, the inspection focused on instances that occurred. Observed that, as a result of this support, a PowerPoint presentation containing the detailed analysis is available. It was noted that no discrepancies were recorded during the validation, indicating a robust process for decision-making.	No exceptions No exceptions No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
9,2	For voluntary actions, confirmations are made through the Custodian's system or by email. For confirmations through the system, one authorized user uploads the response and another approves it.	Inquired with the custody team that counterparty validation of the whether a confirmation is made at the custodian each time this occurs and confirmed the supporting screens validated remains as a supporting document. Inspected the screens from custody for 2024 which contains the following fields: - Registration date - Reference - Issuer - Sanction of the corporate action Observed that, as a result of the transaction confirmation at the custodian, it was determined that confirmations were correctly identified and received from an authorized source. It was confirmed that no discrepancies were recorded in the counterparty validation.	No exceptions No exceptions No exceptions

Control objectives 9
The controls provide reasonable assurance that security positions and cash balances reflected in investment management systems are reconciled completely, accurately, and timely with actual positions and balances.

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
10,1	The custodian team automatically generates a reconciliation between the Aladdin system and Portfolio Net on a daily basis in the "Reconciliation of Positions-Solutions" module. In case any discrepancy is identified, it is investigated and resolved by the Custody Department.	Inquired about the daily automated reconciliation process between the Aladdin system and Portfolio Net. We were informed that the custody team automatically generates this reconciliation in the "Reconciliation of Positions-Solutions" module. Should any discrepancy be identified, the Custody Department is responsible for investigating and resolving it.	No exceptions
		Inspected the daily reconciliation records generated in the "Reconciliation of Positions-Solutions" module for the evaluated period. Reports providing evidence of the automated execution of this process were reviewed. Additionally, records of identified discrepancies were examined, along with evidence of the investigation and resolution carried out by the Custody Department.	No exceptions
		Observed a live demonstration of the automated reconciliation generation in the "Reconciliation of Positions-Solutions" module. The system's ability to identify discrepancies was verified, and in case any arose, the workflow for investigation and resolution by the Custody Department was observed.	No exceptions

Control objectives 10
The controls provide reasonable assurance that client reports and billing are accurate, complete, and provided to clients in a timely manner.

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
11,1	The financial risk team generates monthly reports for mandate clients from the Aladdin system. Validation is performed by the Operations Team in conjunction with the Custody and Accounting Teams	Inquired with the risk team the issuance of reports for the client monthly this occurs and confirmed the excel report remains as a supporting document. Inspect the excel report for 2024 which contains the following fields: - Name of the Investment Fund - Name of the Asset Management-Company - Market Value invested (in MEX PESOS) Observed that, as a result of the validation, it was determined that provide reasonable assurance that customer reporting and billing are accurate, complete, and provided to customers in a timely manner.	No exceptions No exceptions No exceptions
11,2	The Customer Service Advisor distributes the reports to customers at least once a month via email, if any problems are identified, corrections are made prior to the delivery of the report in the Aladdin system.	Inquired with the non-financial risk area about the process for monthly distribution of mandate reports to clients via email. It was confirmed that reports are sent monthly. Additionally, the manual review process for generated reports was described, along with communication with the non-financial risk team for anomaly resolution, and the final verification prior to uploading and sending through the Aladdin system.	No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
		Inspected a selection of monthly mandate report samples for the period from January 1, 2024, to December 31, 2024. These reports generally detail the portfolio, including market value, asset yield terms, Mexican Government bonds, equities, and overall performance. Observed that reports are sent via email by the investment team to service advisors for subsequent distribution to clients. It was validated that no inconsistencies were reported in these reports during the analyzed period.	No exceptions No exceptions
11,3	Before terminating or interrupting the contract earlier than agreed, final fee invoices are generated and prorated by the Financial Risk Team until the termination date. Note: For the period to be evaluated from January 1 to December 31, 2024, there were no terminations of mandate contracts	Inquired with the financial risk team about the process for generating final fee invoices and prorating them until the termination date, in cases of early contract interruption. Inspected the Aladdin software. It was confirmed that, for the period under evaluation (from January 1 to December 31, 2024), there were no mandate contract terminations. This means the control was not triggered during the audit period. Observed interview how the Financial Risk Team would perform the generation and proration of fee invoices in the event of a termination. Although no actual events could be observed in 2024, it was verified that the process for handling such situations is defined.	There were no terminations of investment mandate contracts during the period covered by the report, which was confirmed by inquiry with the Risk Manager and inspection of the Aladdin system output.

Control objectives 11
Application code changes and configuration parameters are initiated as needed, authorized, and operate according to application specifications to (1) produce valid, complete, accurate, and timely processing and data, (2) ensure application control functionality, and (3) support segregation of duties. The network infrastructure is configured as authorized to (1) enable applications and application controls to operate effectively, protect data from unauthorized changes, (3) provide availability for processing, and (4) support segregation of duties.

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
12,1	The primary change control policy is used to guide development staff in designing, testing, and deploying changes to infrastructure and applications.	Inspected the document "Change Control Management Policy in Production Environment" version 2, approved by Roger Rendon – CIO, for the period from January 1 to December 31, 2024, which establishes guidelines to be considered before implementing changes in production, including those related to the applications SIIF and Soluciones, source code, hardware, communications, and scheduled tasks. Validated that the policy establishes that production changes related to Infrastructure and Communications may be managed by IT teams from headquarters. In such cases, the control policies and protocols defined by that entity must be followed. Inspected that the change control policy will be implemented through the "Procedure for Managing Change Control in the Production Environment", supporting compliance and serving as a guide for involved personnel.	No exceptions No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
12,2	Eventually, the application form is submitted by the application stakeholder and approved by the appropriate Department Leader to develop a new program or change an existing program. Note: The Head Office manages the administrator users of the change tool.	Observed the walkthrough of the change control process for the SIIF and Soluciones applications. The process includes reviewing the change request ticket, attached documentation as required by Annex 1, such as the request form, technical sheet, release document, test evidence, and approvals from the business user and technical lead. Validated that the change was carried out and its execution was properly recorded in Jira Inquired about infrastructure changes during the period from January 1 to December 31, 2024, and it was reported that the SIIF application was migrated to AWS infrastructure on November 15 and 16, 2024. Observed the Jira ticket related to the migration project titled "Infrastructure migration to Amazon Web Services," which included all servers, services, applications, databases, and files of the Fondos companies. Observed the impact analysis and list of authorizers, the release document (including the release plan, contingency plan, and impact analysis), system and user testing documents, screenshots of the test execution and approvals were obtained from the technical lead and the application user. Validated, for a sample of changes selected in accordance with the firm's sampling methodology and covering the period from January 1 to December 31, 2024, that tickets were recorded in the change management tool Jira for the applications within the scope of the SOC 1 evaluation: SIIF and Soluciones.	No exceptions No exceptions No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
		Inspected that the required documentation, as defined in Annex 1, was properly attached. The following was observed across all sample items: * Request form: Validated that it includes the classification of the request, subtype, business need, priority, and impact analysis. * Technical sheet: Validated its presence in all applicable cases. * Release document: Validated that all changes included this document, which contains the release plan, contingency plan, and impact analysis. * System and user testing: Validated for all cases requiring them, as per Annex 1, the corresponding formats and supporting evidence (screenshots) were observed. * Approvals: Validated that all changes were approved by both the application user and the designated technical lead. It was validated that these leads are listed in Annex 2 Authorized IT personnel for production change approvals.	No exceptions
		Observed that testing was performed, approvals were granted, and the changes were implemented in the production environment afterward.	No exceptions
		Observed the users with administrative privileges in the Jira tool. Validated that the users with administrative privileges in the tool are appropriately authorized based on their job responsibilities.	No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
12,3	System testing is performed on all programs affected by the requesting departmental or user support group with the assistance of information technology staff in a test environment. Formal test plans are developed to direct the testing effort of the system.	The system testing process for programs affected by departmental or user support group requests was inquired about. We were informed that these tests are conducted in a test environment in accordance with the documents titled "System Testing" and "User Testing," which detail the involvement of the IT Leader personnel. The documentation of formal test plans developed to guide the testing efforts for the SIIF and Soluciones systems was inspected. Records of system tests conducted in the test environment were reviewed, verifying that they involved affected programs and included assistance from IT personnel. Evidence of test execution and the results obtained was examined. The process of conducting system tests in the test environment for the SIIF and Soluciones systems was observed (through a demonstration or review of recent evidence), confirming that formal test plans are utilized and that collaboration with IT personnel is effective in ensuring the quality of changes.	No exceptions No exceptions No exceptions
12,4	Controls associated with the system's change management process: (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 version approver is restricted to selected personnel. This access is provided by Business Unit contacts with management approval.	Inquired about the controls implemented in the system change management process. It was explained to us that these controls are designed to (1) prevent the change owner from also being the approver, and (2) require multiple levels of approval in accordance with Annex 2 of the Change Management Policy.	No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
		The change management policy and procedures for the SIIF and Soluciones systems were inspected. Supporting documents related to change records were reviewed to verify that, in practice, the owner of a change could not also be its approver, and that the required approvals were applied. Email approvals attached to the change tickets were examined. Observed that the approvers in the change management workflow for the SIIF and Soluciones applications hold supervisory or managerial roles, and that the IT approvers are designated through Annex 2 of the Change Management Policy with authorization from the company's CIO.	No exceptions No exceptions
12,5	After system testing, formal approval is obtained from the requester/tester of the requesting user and/or the support group staff involved in the testing to indicate that the changes have been tested and are ready to be transferred to production. Once the test acceptance approval has been received, the change continues to the next approval step, which is performed by the assigned change and version approvers. Version approvers confirm via email that all required documents are stored for those involved in the process and are required to retain the information. Emergency changes will be managed and documented in accordance with the statements in the Change Control Policy.	Inquired about the approval process following system testing and prior to production deployment. It was explained to us that, after system testing, formal approval is obtained from the requester/tester of the requesting user and/or the IT group staff involved in the testing. This approval indicates that the changes have been tested in the prior environments and are ready for production transfer. Once test acceptance approval is received, the change proceeds to the next approval stage, carried out by the assigned change and version approvers. It was verified that the documents supporting the change workflow are complete according to Annex 1 of the Change Management Policy for production, and that these documents are attached in the ticket management tool.	No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
		Inspected a sample of change management tickets and their associated documentation from the corresponding period. Evidence of formal approval from the requester/tester or support group staff indicating test acceptance was validated. Email communications or system records confirming that version approvers verified the storage of all required documents for the relevant stakeholders were also reviewed. For changes with high priority and organizational impact, the impact analysis was validated to ensure compliance with the Change Control Policy. Observed that, for each change in the sample, evidence of implementation and approval prior to production deployment is attached in the ticketing tool.	No exceptions No exceptions
12,6	All required changes or needs to the system are monitored quarterly by stakeholders, and these changes are selected from a sample of the transfer history report to validate the following: (1) each change was appropriate, (2) documentation was retained, and (3) necessary approvals were obtained.	Observed that for the evaluation period from January 1 to December 31, 2024, the quarterly change monitoring not extend to the Soluciones and SIIF systems. EY, through the Blackrock solution's SOC report, verified change management compliance for the Aladdin system.	Identified exception The Monitoring control, which addresses the risk of unauthorized changes, is not applicable to the SIIF and Solutions applications. Refer to the end of this Control Objective section for Management Response and additional procedures performed by Ernst & Young.

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
12,7	Environments, database development and SIIF application and Solutions The Development area requests the restoration of the development environments of the databases and applications to the infrastructure team by email whenever required. This application requires pre-approval from the Technical Development Leader and the Infrastructure area. Infrastructure then performs the restore by obfuscating the data in accordance with the Data Obfuscation Procedure in the case of SIIF and confirms the completion of the request execution via email or Teams. Note: For development environments in the SIIF and Solutions applications, developers have written and read permissions.	Inspected the document "Change Control Management Policy in Production Environment", version 2, approved by the CIO for the period from January 1 to December 31, 2024, which establishes guidelines that demonstrate the existence of segregated development, testing, and production environments. Validated Section 4, "Policy Statement," establishes the existence of segregated environments as part of the change control process, namely: (1) A development environment, where the development team performs technical testing, which must be validated by the responsible lead. (2) A testing or non-production environment, where functional tests are executed to validate changes from a business perspective; and (3) A production environment, where changes may only be implemented following formal approval and review by the Change Control Analyst, thereby reinforcing both functional and environment segregation. Additionally, reviewed the document "Arquitectura, estándares y capacidad tecnológica", which confirms that the company enforces network-level segmentation based on the purpose of each environment. Observed via Microsoft SQL Server Management Studio (SSMS) the existence of segregated development, testing, and production environments at the database level for the SIIF and Soluciones applications. Inquired the functional owner of the application, who also performs development tasks, has access only to the development and testing	No exceptions No exceptions No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
		environments. These access rights allow for the execution of technical and functional testing as needed. Validated access to the production environment is restricted and controlled and is not granted to the development team.	
		Observed that for the lower environments (development and testing) of the SIIF application the database restorations are requested via email. In these cases, approval (Vo.Bo) is required from both the Technical Lead and the Infrastructure Lead, as the restored data must be obfuscated in accordance with the established SIIF procedure. Observed the confirmation of the restore as part of the process.	No exceptions
		Observed that, at the application infrastructure level, each environment (development, testing, and production) has its own AppShare directory, where the SIIF and Soluciones applications are hosted independently within each environment.	No exceptions
		Inspected the document "Procedimiento para la ofuscación de datos" version 3, approved by Executive Direction of Technology for the period from January 1 to December 31, 2024, which establishes guidelines for modifying database information restored from production for use in non-production environments.	No exceptions
		Inspected the SQL data obfuscation script for the SIIF application and validated that it properly masks sensitive information across non-production environments. The script replaces real data with generic values or placeholders, ensuring that no personally identifiable information (PII) is exposed.	No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
		Validated that the obfuscated fields include descriptions, RFCs, emails, passwords, first names, last names, CURPs, addresses, account numbers, beneficiary details, observations, references, authorization codes, internal comments, transaction details, and any other data that could be considered sensitive or personally identifiable. Observed, for the SIIF and Soluciones applications within the scope of the SOC 1 evaluation and for the period from January 1 to December 31, 2024, the list of users with access to the production servers. It was confirmed that all users with such access are duly authorized in accordance with the responsibilities of their respective roles.	No exceptions
12,7,1	Test environments, databases and SIIF application and Solutions The Development area requests the restoration of the test environments of the databases and applications to the infrastructure team by email whenever required, so that later environment can be used to perform tests with end users. This application requires pre-approval from the Technical Development Leader and the Infrastructure area. Subsequently, Infrastructure performs the restoration of the test environments and confirms the completion of the execution of the request by email or Teams. Note: For test environments in the SIIF and Solutions applications, developers and end users have written and read permissions.	Inquired in a walk-through test, were made with the Development and Infrastructure areas regarding database restoration requests for SIIF and Solutions test environments. They reported that prior approval from the Technical Development and Infrastructure leaders is required for restorations. Observed the documents "Policy for Change Control Administration in Production Environment" (version 2) and "Procedure for Data Obfuscation" (version 3) were inspected. These documents establish guidelines for environment segregation (development, test, and production) and the obfuscation of sensitive data in non-production environments, respectively. Inspected that in SQL Data Obfuscation Script for SIIF was inspected, verifying that mass obfuscation was performed on multiple critical tables such as Contract, User, and Promoter. This involved replacing sensitive information	No exceptions No exceptions No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
		with placeholders and validating the inclusion of key fields like emails and passwords, among others, as well as the deletion of records in specific tables. Inspected the Access Permissions and Environment Setup It was observed that in the SIIF and Solutions test environments, developers and end-users possess both write and read permissions. Remote Desktop access to the production console was validated, confirming its documented network location. It was identified that SIIF and Solutions share a common AppShare, but each environment (development, test, and production) has its own independent AppShare directory. Observed that Database Environment Segregation Segregation of database environments for SIIF and Solutions was observed in Microsoft SQL Server Management Studio (SSMS). Functional personnel with development tasks only have access to development and test environments, and access to production is restricted and controlled in accordance with the "Architecture, standards, and technological capacity" diagram, which confirms the application of network level segregation for the SIIF and Solutions applications.	No exceptions No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
12,7,2	Production environments, databases and SIIF application The infrastructure area, at the request of the development team, prepares the production environment. The changes controls that affect the production environments are executed in accordance with the Change Control Policy and Procedure, whose management mechanism of the service lifecycle of the Jira tool.	Inspected the document "Architecture, Standards, and Technological Capacity" was reviewed, confirming that the company applies network level segregation based on the purpose of each environment. It was observed that, at the application infrastructure level, each environment (development, testing, and production) has its own AppShare directory, where the SIIF and Solutions applications are hosted independently within each environment. This validates the segregation of production environments for each of the SIIF and Solutions databases at the level of the shared application directory structure. Observed the segregation of development, test, and production environments at the database level for the SIIF and Solutions applications was observed in Microsoft SQL Server Management Studio (SSMS). Observed the access to Computer Management was reviewed to check the members of the Administrators group and the memberships of the Active Directory groups. For the SIIF and Solutions applications, the list of users with access to production servers for the year 2024 was validated, confirming that all users with such access were duly authorized according to their role responsibilities.	No exceptions No exceptions No exceptions

Control objectives 12
The controls provide reasonable assurance that physical access to data centers and other sensitive areas is restricted to authorized and appropriate personnel.

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
13,1	Access is restricted to the facilities of Principal Fondos de Inversión, S.A. de C.V. Operadora de Fondos de Inversión at the entrances of the buildings and at the doors of sensitive areas within the buildings (e.g., computer rooms) using electromechanical locks controlled by proximity card, with additional configuration for sensitive areas. In the event of a safety device failure, documented mitigation processes are in place. Note: Principal Inversiones' offices are classified by location and sensitive areas: • In Monterrey (Corporativo Valle) are the sensitive areas of Custody, IT, Accounting and Commercial. • The sensitive areas of Financial Risk, Investments and General Management are located in Mexico City (Corporativo Carso).	Inquired about the physical security guidelines for TRIARA's primary and alternate data centers, as well as the physical access policies for the cloud starting in November 2024. The document details measures such as restricted access control, continuous surveillance with over 100 cameras, and 24/7 monitoring. Inspected the physical access controls during the walk-through test on May 2, 2025. The controls applicable to corporate buildings and data centers were explained, with sensitive areas classified by location. In Monterrey (Corporativo Valle), the sensitive areas include Custody, IT, Accounting, and Sales. In Mexico City (Corporativo Carso), the sensitive areas are Financial Risk, Investments, and General Management. Observed the existing physical security measures through photos of corporate entrances provided in the documentation. These visuals demonstrate the effectiveness of the implemented security protocols and reinforce the commitment to maintaining a secure environment for sensitive operations.	No exceptions No exceptions No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
13,2	The Infrastructure Systems team conducts a semi-annual email review of users who are granted access to the data centers	Inquired about the physical security guidelines for TRIARA's primary and alternate data centers, as well as the physical access policies for the cloud starting in November 2024. The document outlines measures such as restricted access control, continuous surveillance with over 100 cameras, and 24/7 monitoring. Inspected the semiannual review process for permanent access at the TRIARA data center. It was validated that the TRIARA data center provider sends the list of authorized users with permanent access to the infrastructure area via email for review. Observed the verification by the area, which contains authorized users with permanent access. Observed that the entity revalidates these users, confirming whether they remain active or if any changes are required. These users are part of the infrastructure area, ensuring that access is appropriately managed and aligned with security protocols	No exceptions No exceptions No exceptions
13,3	Physical accesses are removed when a user is unsubscribed. A notification is made to the Infrastructure System team to proceed with the update in the proximity card system to disable the cards of terminated employees.	Inquired about the process for removing physical access when a user is unsubscribed. Validated that the review focused on the physical access process, referencing the established guidelines for access control. For this control, temporary access for scheduled visits is reviewed, requiring a request to be filled out in a specific format before attending the data center.	No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
		Inspected the physical access controls during the walk-through. The physical security guidelines were reviewed, detailing measures such as restricted access control and 24/7 monitoring. Observations from the photos showed the biometric door closures at the corporate locations of Carso and Valle, highlighting the security measures in place to ensure effective access control. Observed that the use of standardized forms for scheduled visits was observed, indicating the implementation of formal procedures for temporary access management. Additionally, the validation of approvals for professionals with permanent access to the data center was noted, reinforcing control over those with continuous access privileges. Finally, it was observed that the administration of administrator users for the proximity card system is handled by authorized Access Control Technicians, suggesting a segregation of duties in the management.	No exceptions No exceptions

Control objectives 13

The 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 modifications and support segregation of duties.

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
14,1	Policies, standards, and procedures are set in all major information resources to set requirements for how to configure security components and logical security controls.	Inquired in the document 'Access Control Policy and Procedure', effective for the period from January 1 to December 31, 2024. This policy details the regulations for assigning access rights to information in business applications (including SIIF, Solutions and Aladdin) and various IT services (such as databases, networks, file repositories, e-mail and VPNs). The objective of this policy is to ensure adequate, efficient, consistent and auditable access, aligning with the company's global strategy and current regulations. Inspected the documented flowchart 'Access Removal Flowchart', confirming that the procedure requires the Collaborator to manage the pertinent authorizations and send the ABC request to CDS, who validates and manages the request, documenting the service in 'track it'. Observed that ServiceNow is the formally designated ticketing tool to manage all requests related to provisioning, modifying and deprovisioning access for SIIF, Solutions and Aladdin applications.	No exceptions No exceptions No exceptions
14,2	For account provisioning and deprovisioning, the ABC process is carried out when the requesting user submits a request form approved by the Department	Inquired in the document 'Access Control Policy and Procedure', effective for the period from January 1 to	No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
	Head to the Support Center that validates that the access request is appropriate according to the job functions. In the event that specific access rights are needed, the Support Center notifies the Corporate Infrastructure Team for appropriate treatment. Note 1: Approval for the provisioning of accounts is made by the Head of Department, based on his or her criteria of expertise. Note 2: For Solutions, the provisioning and deprovisioning flow applies to the application, not to the databases. This is because "Database as Filesystem" (DBaaS) is used, which allows access to the file system interface to users in the support and treasury center.	December 31, 2024. This policy details the regulations for assigning access rights to information in business applications (including SIIF, Solutions, and Aladdin) and various IT services (such as databases, networks, file repositories, e-mail). The objective of this policy is to ensure adequate, efficient, consistent, and auditable access, aligning with the company's global strategy and current regulations. Inspected for user extraction from SIIF and Solutions, as well as active payroll. A list of active and retired professionals or external personnel from Principal Fondos was requested. For each, the creation or deletion ticket with its approval trail, the ABC format, the immediate supervisor's approval flow with the application owner including the 2024 role and profile (via approval email), direct prints from the applications and/or databases with created, deleted, and retired users, and Annex 1 of Responsible Parties and Authorizers valid for the period were requested. Inspected the documented flowchart 'Access Removal Flowchart' was inspected, confirming that the procedure requires the Collaborator to manage the pertinent authorizations and send the ABC request to CDS, who validates and manages the request, documenting the service in 'track it'. The ABC format specifying the permissions or roles being granted or revoked was also inspected. Observed for the ServiceNow tool, the printout of users with access for Principal Fondos and a supporting	No exceptions No exceptions No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
		document for said access were requested. For DA (Operating Systems), a list of tickets with their approvals was requested of the approval process by the requesting user's manager was sought to validate the information source for assigned user roles. Observed that, given the DBaaS model, provisioning and deprovisioning controls must be designed and applied specifically for the application layer, as this is the primary interface through which users (from support and treasury) interact with the data. It is crucial to observe that while the database itself is not the direct point of access control for end-users, database security remains fundamental at the infrastructure level for proper functioning and data integrity.	No exceptions
14,3	A monthly technical review is conducted to identify employee terminations to disable accounts or access rights in applications and/or systems (SIIF, Solutions, Aladdin). Third parties granted access rights are also considered within the review.	Inquired in the document "Procedimiento de Revisión de Terminación de Usuarios Mensual (Monthly Terminated Review) " Version 1 approved by Chief Information Officer for the period from January 1 to December 31, 2024, whose objective is to have a documented and structured process that identifies active user accounts that have not been deregistered from the applications or systems that support the service within the scope, ensuring that any deviations detected are addressed. Inspected that the procedure and flowchart reflect that the process starts with the OSI's request for the active payroll	No exceptions No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
		user reports, validated that the Support Center sends the report of active users of external consultants with a "Vo.Bo", and the System Administrator sends the report of active users of the applications (SIIF, Solutions, Aladdin). Observed that the OSI is responsible for obtaining the list of the repository of the Human Resources (HR) interface related to internal collaborators and compares the internal active users and external active consultant users with the active users within the applications, validated that the differences found are reported, and if there are active users in the applications that do not appear as internal or external active users, the User Manager must determine if there is a business need to maintain such active access, validated that in the event that a user detected as terminated is not terminated, the User Manager must notify the OSI. If there are detected users that do not have a termination instruction executed, it was observed that the System Administrator executes the pending terminations of reported users and notifies the OSI. Finally, it was observed that the System Administrator generates and sends the evidence with the reflected changes to the person responsible for the application and/or OSI, and the review is documented, a checklist is managed and stored for future consultation. Observed that for the period from January 1 to December 31, 2024, there were no deviations of reported users that generated action plans.	No exceptions No exceptions
14,4		Inquired in a walkthrough test with Project Leader TI, confirming that the system settings for the SIIF and	No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
	Accounts with no registration activity for a period longer than 90 days are automatically blocked or disabled.	Solutions applications are configured to automatically lock or disable user accounts after 90 days of inactivity. Inspected the access management control for the SIIF and Solutions applications, which includes functionality that automatically locks or disables user accounts that have not logged activity for a period exceeding 90 days. This measure enhances security by ensuring that inactive accounts do not remain accessible. Observed that the administrators of Active Directory for the Solutions application are Access Control Supervisor and his teams. Additionally, it was noted that no account lockouts of this type have occurred for any application, demonstrating the effectiveness of the control in place.	No exceptions No exceptions
14,5	User access review is conducted at least annually by the IT Department in conjunction with process owners for access rights granted to critical applications. If discrepancies are identified, they are evaluated to define whether or not access should remain. Note: For the Aladdin application, the review is done semi-annually through mail.	Inquired about the document "Procedimiento de Revisión de Derechos de Acceso de Usuarios (Entitlement Review)" for the period from January 1 to December 31, 2024. The objective of this document is to establish a structured process for periodic review by application managers of authorized user roles and access rights, aligning with the company's overall strategy. Inspected the information provided regarding the user access control review process. Validated that this process is conducted annually for the SIIF and Solutions applications, and semi-annually for Aladdin. Observed that the CIO requests user reports and profiles for the different applications from the access control team	No exceptions No exceptions No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
		or the DBA, as applicable. These reports are compiled in an Excel template and sent to the application owners for review and validation of access. If any deviations are identified, a case is triggered and handled through an ABC ticket. It was noted that no deviations occurred for the applications in scope during the evaluation period. Observed the reviews conducted during the 2024 period for the Aladdin, SIIF, and Solutions applications. The step-by-step process was demonstrated, starting from the extraction of users, followed by the IT department sending the information to the owner, who then reviews the access rights.	No exceptions
14,6	Windows security settings are reviewed quarterly by Information Security and Risk. Configurations that do not meet defined security standards are reported to the CIO Working Group	Inquired that quarterly, the Information Security team of the holding reviews Windows server configurations and generates a compliance indicator report, which is then communicated to the CIO Working Group. Inspected about the document "Políticas y estándares para la identificación y autenticación" Version 1, approved by the Chief Information Officer for the period from January 1 to December 31, 2024. The objective of this document is to define the mandatory access management and authentication measures necessary to protect the privacy, security, and confidentiality of company resources. Observed the process and results of the validation for a selection of quarterly samples of Windows server security	No exceptions No exceptions No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
		parameter reviews, conducted by the holding company's Information Security area, were inspected. This included reviewing reports containing specific metrics that showed a high level of compliance, with compliance percentages consistently remaining above 99% and no areas for improvement identified, indicating consistent compliance across the quarters. It was further validated that the results of these reviews and the compliance status are reported to the CIO Working Group. Observed that the security configurations for Windows in the SIIF and Solutions applications include a password policy requiring a minimum of 8 characters, a maximum expiration date of 60 days, and the complexity requirement of having at least one (1) character from at least three (3) of the four (4) character categories (A-Z, a-z, 0-9, special characters). The configurations were also reviewed directly from Active Directory, confirming their alignment with the established policy. It was observed that there were no areas of opportunity, and compliance was maintained in the reviewed quarters according to the compliance reports. Observed that the 'ServiceNow' tool is utilized as a central platform for managing logical access flow and user administration. It was noted that there is control over audit traceability, including the identification of actions such as ticket or field deletion, which is crucial for maintaining a complete audit trail. Furthermore, it was observed that user administration through the Support Center has a defined team with specific roles (Supervisor, Technician, Analyst, Manager), suggesting a segregation of duties in the access management process.	No exceptions No exceptions

Control objectives 14

The controls provide reasonable assurance that application and system processing is authorized and executed completely, accurately, and timely; and that deviations, issues, and errors are identified, tracked, recorded, and resolved completely, accurately, and timely. The controls provide reasonable assurance that data and application backups are made to allow restoration of applications and processing in case of data or application destruction.

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
15,1	Principal Fondos de Inversión, S.A. de C.V. Operadora de Fondos de Inversión actively monitors networks, services, operating systems and databases in the system and information processing to identify incidents. When identifying incidents, the user is responsible for reporting the incident to the Support Center, which generates the ticket and assigns it to the appropriate level based on severity for a timely response.	Inspected the document "Protocol for Global IT Incident Management in Mexico" for the period from January 1 to December 31, 2024. This procedure establishes a unified protocol for the detection, classification, response, escalation, and communication of incidents, and includes clearly defined procedures, responsibilities, a process flowchart, and severity levels. Observed that two predefined forms "PI Mexico Sev 1 Form" and "PI Mexico Sev 2 or Info Form" are available for registering Severity 1 and Severity 2 incidents; otherwise, the default form is used. The ticket related to SIIF was reviewed, and it included traceability of the incident, description, and resolution. Observed that incidents affecting the performance of networks, services, operating systems, and databases, as well as information processing, are recorded in order to identify issues. xMatters is the incident management tool used to register incidents related to the three applications within the scope: SIIF, Soluciones, and Aladdin. Observed for the period from May 1 to December 31, 2024, a sample of incidents affecting the performance of networks, services, operating systems, databases, and information processing was observed (selected according to the firm's sampling methodology). It was confirmed that tickets were properly registered in the xMatters tool and met SLA requirements based on defined severity levels.	No exceptions No exceptions No exceptions No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
		Validated that the user reports the incident to the Support Center, which is responsible for generating the ticket and assigning it to the appropriate level based on its severity for a timely response. Observed that the users with administrative privileges in the xMatters tool are safeguarded and monitored by corporate headquarters. It was verified that these users possess appropriate authorization aligned with their defined job responsibilities. Observed during a walkthrough test conducted on April 22, 2025, that the extraction of tickets from the incident management tool for the period from January 1 to April 30, 2024, does not retain the information in said tool, this is due to restrictions associated with the type of license contracted.	No exceptions Identified exception Due to restrictions associated with the type of licensing contracted, the xMatters tool does not retain information for a period of more than one year. Refer to the end of this Control Objective section for Management Response and additional procedures performed by Ernst & Young.
15,2	Servers are backed up daily and replicated to the disaster recovery data center. Note 1: By November 15 and 16, 2024, the Backup process changed to AWS. Note 2: For the period to be evaluated, no backup restores were requested for the SIIF and Solutions applications.	Inspected the document "Backup and Data Restoration Policy" version 5, approved by the Deputy Director of Infrastructure and Communications for the period from January 1 to December 31, 2024. The policy aims to back up the logical content of the SIIF and Soluciones application systems in a reliable and secure manner. It was identified that the Technology Infrastructure area fills out the Backup Log with the daily execution date, servers, record of successful execution, and verification.	No exceptions No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
		Observed the production backup configuration in IBM Spectrum Protect for the Soluciones application and validated that: • Incremental daily backups are executed on the Data Center servers. • Backup retention is performed every eight days on the Virtual Machine (VM) system, with eight days of retention at the file level on Windows, and twenty-one days on Linux. Observed the production backup configuration in AWS for the SIIF application, and identified that: • Incremental backups are executed daily for the period from November 16 to December 31, 2024, according to the migration. • Backup retention is performed every fourteen days regardless of the operating system. • The S3 Bucket configuration in AWS was validated, confirming its redundancy across multiple regions. Observed that the Commvault tool is configured and aligned with AWS and validated the backup frequencies according to policy. Observed that in the IBM system, administrator users are configured and monitored by the infrastructure area. Observed that in the AWS Master module, administrator users are configured and monitored by the corporate headquarters, who manage the system.	No exceptions No exceptions No exceptions No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
		Observed that, for the evaluated period, no backup restoration requests were made for the SIIF and Soluciones applications through the support tool.	
15,3	When registering and coding new Counterparties in Aladdin, these must be approved by the Risk Committee. In addition, the Financial Risk Department conducts a review on a quarterly basis to confirm accuracy between counterparties on the Approved Counterparties List and the Aladdin system. Any concerns or discrepancies identified are investigated and resolved.	Inquired about the process for registering and coding new counterparties in Aladdin. The Financial Risk Department explained that new counterparties must be approved by the Risk Committee. They also conduct a quarterly review to ensure accuracy between the Approved Counterparties List and the Aladdin system. Any identified concerns or discrepancies are investigated and resolved. Inspected documentation of authorized counterparties in Aladdin and disclosures made to the Risk Committee. We reviewed records of the quarterly reviews performed by the Financial Risk Department. To validate operational effectiveness, we selected a random sample of two periods/months. Verified counterparty disclosure attributes and fund ratings performed by the investment team. Observed the monitoring of authorized counterparties from Aladdin and the disclosures to the Risk Committee. We confirmed that the quarterly review process is conducted and that discrepancies, if any, are investigated and resolved.	No exceptions No exceptions No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
15,4	A daily reconciliation is made between PortafoliosNet and the portfolio provided by the custodian, positions are composed as cash. In case any discrepancies are identified, they are investigated and resolved by the Custody Department. Conciliations are recorded through a .xls and the Custodian team reviews and approves the reconciliations (signed or electronically or by email).	Inquired with the custody team about the daily reconciliation process between PortafoliosNet and the portfolio provided by the custodian, where positions are composed as cash. The team confirmed that the reconciliation is performed daily, and that support is provided via email. Should any discrepancies be identified, they are investigated and resolved by the Custody Department. Reconciliations are recorded through an .xls file, and the Custody team reviews and approves these reconciliations (signed electronically or by email). Inspected the evidence of daily reconciliations in .xls format generated for a sample from January 1 to December 31, 2024. We reviewed the approval records from the Custody team, email confirmations, to ensure that the review and approval were performed in a timely manner. Furthermore, we examined the details of any identified discrepancies, if any, and the documentation of investigations and resolutions carried out by the Custody Department, to verify the completeness and effectiveness of the tracking and correction process. Observed that, as a result of this monitoring, the reconciliations are sent to the custody team via email, and confirmation of their submission was provided. Furthermore, it was observed that no discrepancies were recorded in the email distribution or material differences to report.	No exceptions No exceptions No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
15,5	The configuration of the jobs is executed from the change management process through the Jira tool, in the release format the script to be executed is described to be tested in the development and test environments, and then the infrastructure team implements in the SIIF production environment through SQL Server. Note 1: On November 15 and 16, 2024, the migration to AWS infrastructure for the SIIF application was carried out and all jobs were reconfigured. Note 2: For Solutions there are no jobs, Database as Filesystem is used.	Inspected the document "Change Control Management Policy in Production Environment" version 2, approved by the CIO for the period from January 1 to December 31, 2024, which establishes that the configuration of production jobs for the SIIF application database is executed through the change management process. Observed that the job configuration for the SIIF application is performed following the change management process through the Jira tool. It was identified that the release format includes the procedures to carry out the migration of AWS, including a section for importing jobs into the SIIF database. Testing is conducted in development and testing environments, and subsequently, the infrastructure team executes in the production environment via SQL Server. Observed that, during November 16 and 17, 2024, the SIIF application was successfully migrated to the AWS infrastructure. As part of this migration, scheduled jobs were configured in the databases using the Lift and Shift strategy. It was validated that the configuration and execution followed the flow established in the organization's change management procedure. For a selected sample of these jobs, the corresponding scripts were reviewed via SQL Server. These scripts contain commands for data manipulation and processing tasks, as well as instructions for report generation and automation of internal processes. It was validated that the configuration parameters of each job are correct, properly controlled, and that their implementation was authorized and approved according to internal procedures.	No exceptions No exceptions No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
		Observed the configuration of a SQL Server job executed in the database to purge the SQL Server job history every 30 days. Observed that for the Soluciones application, a Database as Filesystem structure is implemented, which consists of a file system to organize and store data. According to the architecture diagram, it was validated that under this architecture there is no intrinsic logic to execute scheduled tasks.	No exceptions No exceptions
16,1	At least once a year, the Investment Department qualitatively and quantitatively assesses the service levels provided by counterparties throughout the terms of the mandates to review the fairness of the allocation process.	Inquired with the investment team about the process for validating counterparty service through a quantitative and qualitative analysis. The team confirmed that this assessment is performed at least once a year and that the Excel analysis file serves as a supporting document. It was explained that this evaluation aims to review the fairness of the allocation process throughout the terms of the mandates. Inspected the quantitative and qualitative analysis file for 2024. This file contains the following fields: Counterparty Name, Service Type, Service Quality (Qualitative), Transaction Volume (Quantitative), Average Response Time (Quantitative), Number of Reported Incidents (Quantitative), Problem Resolution (Qualitative), and Additional Comments. This data is analyzed by the investment team to determine each counterparty's performance.	No exceptions No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
		Observed that, as a result of the counterparty analysis, the quality of the service levels provided is determined. It was validated that no discrepancies were recorded in the counterparty validation, indicating a consistent process for evaluating service provider performance.	No exceptions
16,2	The Financial Risk area, in conjunction with the investment area, reviews daily that the investment portfolio complies with the investment regime, the deviations detected that break the regime of the assignment procedures through the Aladdin dashboards, are escalated to the Compliance Department, investigates and resolves the identified exceptions.	Inquired with the Financial Risk and Investment areas about the daily process of reviewing the investment portfolio's compliance with the established investment regime. They explained that deviations that break the assignment procedures' regime are detected through Aladdin dashboards and escalated to the Compliance Department, which is responsible for investigating and resolving the identified exceptions.	No exceptions
		Inspected evidence of the daily reviews of investment regime compliance. evaluated period was selected. Records of detected deviations, email communication to the Principal compliance team, and documentation of investigations and resolutions for items violating the regime were reviewed. Furthermore, "Net Portfolios" database was extracted to verify the existence and accuracy of the information.	No exceptions
		Observed, the review of investment regime compliance and the email sent to the Principal compliance team. It was verified how deviations are identified in the Aladdin dashboards. During this observation, no deviations requiring escalation, investigation, or resolution were detected, indicating effective regime compliance in the observed period.	No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
16,3	A strategy meeting is held monthly with the investment team, risks, the CEO, the leaders of each area (if applicable), as a result of this process the Investment team communicates the strategy through a presentation with the trading and the investment portfolio on the positions of the mandates attending the monthly meeting of the Committee, the follow-up of which is agreed at the session.	Inquired with the risk team that validation of the strategy on mandate positions and confirmed that the presentations validated remains as a supporting document. Inspected the presentations for the months of 2024 which contains the following fields: - Foreign Ownership - Nominal and Real Curve - Fund Competition Observed that, as a result of the meet, it was determined that provides reasonable assurance that block orders are allocated to customers fairly. It was confirmed that no discrepancies were recorded in the counterparty validation.	No exceptions No exceptions

Control objectives 15
The controls provide reasonable assurance that block orders are allocated to customers in a fair manner.

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
16,1	At least once a year, the Investment Department qualitatively and quantitatively assesses the service levels provided by counterparties throughout the terms of the mandates to review the fairness of the allocation process.	Inquired with the investment team about the process for validating counterparty service through a quantitative and qualitative analysis. The team confirmed that this assessment is performed at least once a year and that the Excel analysis file serves as a supporting document. It was explained that this evaluation aims to review the fairness of the allocation process throughout the terms of the mandates. Inspected the quantitative and qualitative analysis file for 2024. This file contains the following fields: Counterparty Name, Service Type, Service Quality (Qualitative), Transaction Volume (Quantitative), Average Response Time (Quantitative), Number of Reported Incidents (Quantitative), Problem Resolution (Qualitative), and Additional Comments. This data is analyzed by the investment team to determine each counterparty's performance. Observed that, as a result of the counterparty analysis, the quality of the service levels provided is determined. It was validated that no discrepancies were recorded in the counterparty validation, indicating a consistent process for evaluating service provider performance.	No exceptions No exceptions No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
16,2	The Financial Risk area, in conjunction with the investment area, reviews daily that the investment portfolio complies with the investment regime, the deviations detected that break the regime of the assignment procedures through the Aladdin dashboards, are escalated to the Compliance Department, investigates and resolves the identified exceptions.	Inquired with the Financial Risk and Investment areas about the daily process of reviewing the investment portfolio's compliance with the established investment regime. They explained that deviations that break the assignment procedures' regime are detected through Aladdin dashboards and escalated to the Compliance Department, which is responsible for investigating and resolving the identified exceptions.	No exceptions
		Inspected evidence of the daily reviews of investment regime compliance. evaluated period was selected. Records of detected deviations, email communication to the Principal compliance team, and documentation of investigations and resolutions for items violating the regime were reviewed. Furthermore, "Net Portfolios" database was extracted to verify the existence and accuracy of the information.	No exceptions
		Observed, the review of investment regime compliance and the email sent to the Principal compliance team. It was verified how deviations are identified in the Aladdin dashboards. During this observation, no deviations requiring escalation, investigation, or resolution were detected, indicating effective regime compliance in the observed period.	No exceptions

Control ID	Description of Principal's control	Procedure developed by EY	Test Result
16,3	A strategy meeting is held monthly with the investment team, risks, the CEO, the leaders of each area (if applicable), as a result of this process the Investment team communicates the strategy through a presentation with the trading and the investment portfolio on the positions of the mandates attending the monthly meeting of the Committee, the follow-up of which is agreed at the session.	Inquired with the risk team that validation of the strategy on mandate positions and confirmed that the presentations validated remains as a supporting document. Inspected the presentations for the months of 2024 which contains the following fields: - Foreign Ownership - Nominal and Real Curve - Fund Competition Observed that, as a result of the meet, it was determined that provides reasonable assurance that block orders are allocated to customers fairly. It was confirmed that no discrepancies were recorded in the counterparty validation.	No exceptions No exceptions

SECTION V

Other Information Provided by the Service Organization

Other Information Provided by The Service Organization

Management's response to identified deviations

- Control ID 12.6 Management Response: For the year 2024, the control was not designed as planned. Although it was expected to be operational for the corresponding 2024 review, internal challenges prevented its implementation. We confirm that, starting in the second quarter of 2025, Principal Fondos de Inversión's systems will be integrated into the quarterly review, in accordance with our agreements.

- Control ID 15.1 Management Response: The Technology area will implement a process for the periodic export of complete incident ticket data from xMatters. This data will be securely archived in an alternative repository that guarantees its integrity, immutability, and long-term custody.

Controls not evaluated

It's important to note that this report includes other information provided by the management of Principal Fondos de Inversión, S.A. de C.V., Operadora de Fondos De Inversión, Principal Grupo Financiero which is presented in the section titled 'Other Information Provided by the Service Organization' Section V. While we've read this information to identify material inconsistencies with the system description, management's assertion/statement, or our report, it's crucial to understand that this information is not part of our assurance engagement, and therefore, we haven't performed audit procedures or expressed an opinion on it.

Specifically, the following activities were reviewed solely to understand their processes, and weren't evaluated for controls within the scope of this SOC 1 Type 2 report:

1. Privacy Program
2. Business Continuity Program
3. Disaster Recovery Program
4. Information Security Program
5. Record Retention Policy

APPENDIX A.
Selection Table

Selection Table

For the request for evidence under selection, the table presented below was used.

Nature of Control and Frequency of Performance	Minimum Number of Items to Test (Note 2)
Manual control or manual portion of ITDM control, performed daily or many times per day (Note 1)	25 (or 60, if only one control per category of risk is selected to be tested)
Manual control or manual portion of ITDM control, performed weekly	5
Manual control or manual portion of ITDM control, performed monthly	2
Manual control or manual portion of ITDM control, performed quarterly	2
Manual control or manual portion of ITDM control, performed semi-annually	Judgmental
Manual control or manual portion of ITDM control, performed annually	1
Application control or automated portion of ITDM control	Test once for each type of transaction and processing alternative, if supported by effective IT general controls (that have been tested); otherwise, sample items are selected based on judgement.
IT general controls	Follow guidance above for manual and automated aspects of ITGCs

Contact Our Investment Team

Gustavo E Cubides
Partner | FSO FAIT LAN
Cel. +57 3153080906
Gustavo.E.Cubides@co.ey.com

Martha Guerrero
Executive Director
Cel. +57 3176645275
Martha.C.Guerrero@co.ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society, as well as to build trust in capital markets.

Through data and technology, EY's diverse and inclusive teams, located in more than 150 countries, provide trust through assurance and help clients grow, transform and operate.
Through a multidisciplinary approach to assurance, consulting, legal services, strategy, tax and transactions, EY seeks to empower its teams to ask better questions to find new answers to the complex issues facing our world today.

ey.com