GRUPO SUPERVIELLE



Lines of Defense and Regulatory Compliance Policy

Grupo Supervielle S.A.

December 16, 2022

TABLE OF CONTENTS

1. INTRODUCTION..... 3
2. GOVERNANCE 4
3. ENFORCEMENT 4
4. PROHIBITIONS..... 4
5. OBLIGATIONS RELATED TO RISK MANAGEMENT 4
6. OBLIGATIONS RELATED TO REGULATORY COMPLIANCE 5
7. INQUIRIES RELATED TO REGULATORY COMPLIANCE..... 10
8. COORDINATION AMONG THE THREE LINES OF DEFENSE 10
9. SPECIAL CONTROLS..... 10
10. SAFETY TEST 10
11. ETHICS & VALUES LINE..... 11

1. INTRODUCTION

Grupo Supervielle promotes an effective risk management framework based on the three lines of defense model proposed by COSO (Committee of Sponsoring Organizations of the Treadway Commission). It is essential that all employees know what their role is, their specific functions, the risks that their activity and/or decisions entail, and how to mitigate them.

The three lines of defense model purpose is to define the employees´ role in the organization when identifying, managing, and effectively addressing business risks. It distinguishes three essential aspects:

Risk ownership, risk supervision and control, and independent risk guarantee / assurance.

The three lines of defense model has the following functions:

First line of defense

It is the processes owner in charge of risk management, design, and implementation of the internal control system. It is made up of business executives, including, among others, Experience Leaders, Tribe Leaders, and Product Owners (POs), Digital Marketing and CX-UX (Customer and User Experience) COEs, IT Architecture, Advanced Analytics, and Data and Digital Transformation.

Second line of defense

Oversees effective risk management and control. Proposes policies in line with best practices and risk appetite thresholds, and performs regular monitoring. It is made up of the areas that carry out support functions (among others, Risks, Compliance, Cybersecurity, AML, and the Cybersecurity COE).

Third line of defense

Evaluates efficiency of the organization's defense barriers (first and second). Carries out independent assurance of risk quality and control. Must analyze whether procedures and policies are adequate and if they are followed, if risks are well assessed and if the organization operates within appetite parameters set by the Board of Directors. It is made up of Internal Audit.



Copyright 2020 by The Institute of Internal Auditors, Inc. All rights reserved.

2. GOVERNANCE

The Board of Directors of Grupo Supervielle will be the body in charge of reviewing and modifying this policy with the recommendations of the Ethics, Compliance & Corporate Governance Committee.

The Compliance Department will be in charge of executing this policy.

3. ENFORCEMENT

This policy applies to Grupo Supervielle and its related companies and the reference to Grupo Supervielle in this document will include each of its related companies. Failure to comply may imply labor sanctions. This policy and all obligations established herein must be aligned with the agility premise established in the current operating model.

4. PROHIBITIONS

Affectation of the risk control system established by Grupo Supervielle is prohibited, either by making decisions outside the attributions of employees, by the decision to fail to comply with the applicable regulations or by any other action of any nature.

Failure to comply with this policy may imply labor sanctions.

5. OBLIGATIONS RELATED TO RISK MANAGEMENT

Obligations of employees in relation to this risk management scheme are detailed below.

Risks Structure and Knowledge

Employees have the obligation to know their role and attributions within the organizational structure to which they belong, as well as the risks inherent to the functions they perform and the way to mitigate them, including non-compliance risks according to what is established in item 6 of this policy (Obligations Related to Regulatory Compliance).

Powers and decision making

Employees must know what their powers and attributions are and may only make decisions within them and with the approval levels required for each case.

Decisions outside of powers. Opinion of specialist areas. Governance: Operational Risk Committee and Ethics, Compliance & Corporate Governance Committee

If employees consider it necessary to make a decision outside of their powers or attributions or faced with the risk of possible regulatory non-compliance, they must submit it to the Operational Risk Committee or corresponding forum, as the case may be, explicitly reporting the risks that arise of the decision and (if any) the risk that the decision may result in a regulatory breach or change to an existing process or control. Before submitting the decision to

the Operational Risk Committee or the corresponding forum, they must have the opinion of specialists or support areas. Committee members must identify risks involved in the proposed decision and assess the risk to be assumed. At least the following areas will participate in the Operational Risk Committee: Legal, Compliance, Internal Control, Operations, SOX, and business officials.

Any decision that may involve a conflict of interest, ethical issues, donations, contributions to public bodies, must be channeled through the Ethics, Compliance & Corporate Governance Committee.

Any decision that is outside the powers of the Operational Risk Committee or the Ethics, Compliance & Corporate Governance Committee must be submitted to the Risk Management Committee.

Warning of Violations

If an employee becomes aware of a breach of any internal or external regulation or of a failure in controls, they are obliged to immediately notify support areas that make up the second line of defense (Risks, Compliance, AML, as appropriate), to the Audit Department or through the Ethics & Values Line.

Risk Aligned Objectives

Actions that are within the risk appetite defined by the Board of Directors are rewarded. It is the responsibility of each leader to set objectives for their employees that are within this appetite and that do not jeopardize the risk control defense and management system implemented by Grupo Supervielle. Failure to comply with this section may be taken into account when defining the employee's remuneration scheme.

Risk Mitigation

All employees must be aware of the risks inherent to their functions and the internal and external regulations that regulate their processes and mitigate the risks that arise in the performance of their functions.

6. OBLIGATIONS RELATED TO REGULATORY COMPLIANCE

All employees of Grupo Supervielle must know the rules that apply to the functions they perform and the sector in which they carry out their activities.

It is the responsibility of the first line of defense (Experience Leaders, Tribe Leaders and Product Owners) to know, implement and comply with applicable regulations. This responsibility must be established in the Functions Handbook and in the job description of employees who assume these roles.

Obligations of the areas related to regulatory compliance are set out below:

Knowledge of standards

The first line of defense (Experience Leaders, Tribe Leaders and Product Owners, process owners and product managers) has the responsibility of knowing all regulatory norms that impact on products that concern them and keeping up-to-date (through the service of "Regulatory Alerts" provided by "Normas Financieras.com" of Microbas S.R.L. available at the Bank) as well as ensuring that processes are updated at all times.

Specialist areas (Legal, Compliance, Operations, Technology, Accounting, Taxes, AML, Risks, HR, among others) are in charge of implementing regulations that are their responsibility and that have been defined

within their responsibility, as well as defining the second line controls in the event that they were necessary or on the recommendation of Internal Audit.

People responsible for a process must manage its registration in the list of norms distribution "Alertas Normativas" (Regulatory Alerts).

Notification of new standards and implementation monitoring

The Compliance Department is in charge of notifying the different areas of new standards issued by regulators, paying special attention to those that regulate aspects of products or protection of users of financial services. Will carry out monthly monitoring of their implementation, which will be reported to the Board of Directors and Senior Management. Standards issued during the week will be published weekly in Workplace - Compliance.

Rules that regulate specific aspects such as Comex, Exchange, Accounting, Taxes, Solvency Liquidity, Cybersecurity, Fraud, aspects related to the scope of Cybersecurity COEs, IT Architecture, Advanced Analytics / Data, Digital Transformation, Digital Marketing and CX UX, etc., will be implemented by these same specialist areas that will issue an opinion and distribute it to the sectors affected by the regulations, if applicable.

It should be noted that notification of new regulations issued by the regulators by the Compliance Department does not supersede the obligation of the first line and of the specialist areas to know through the Regulatory Alerts system the regulations that apply to their processes.

Application/Implementation of standards. Regulation type

All employees must know and apply/implement rules, both internal and external, that regulate their functions following interpretation guidelines established by specialist areas.

For their application/implementation, they must request the opinion of corresponding specialist areas and must ensure that said implementation is executed in compliance with all regulatory, functional, technological, etc. requirements.

In the event of any doubt about the application, implementation and/or interpretation of applicable regulations, the Legal Affairs Department, or the Compliance Department (as the case may be) should be consulted.

The Legal Affairs Department will issue opinions on implementation of laws and regulations of regulators (BCRA, CNV, UIF, SSN and any other that issues regulations applicable to Grupo Supervielle's businesses), especially those related to products and services.

The Compliance Department will respond to inquiries about regulations issued by regulators (BCRA, CNV, SSN, DNPDP) regarding effective dates, registrations according to Expansión de EF, protection of users of financial services, registration of databases, regulatory requirements, and reporting regimes. Likewise, they will carry out interpretation of internal policies under their responsibility and supervision.

For the purposes of this Policy, we classify standards into two types:

Cross regulation. Standards that imply the development of products or services, standards that impact the relationship with clients

"Cross Regulation" is defined as a regulation originated by any of the external control entities (BCRA, CNV, AFIP, SSN, FIU, Laws, Decrees) whose mandatory objective is the implementation within an established term of an innovation or modification that involves several areas, mobilizes important bank resources and/or requires special

coordination and monitoring for its effective completion.

For the implementation of these standards, in the event that they involve and impact different areas of the bank, the person responsible for application / implementation must coordinate with the Processes Department creation of a team to carry out the corresponding follow-up. The team must have the presence of the Product Owner, Legal, Compliance, Risks, Processes, Systems, Responsible for Users of Financial Services, and any other area that is necessary.

If the standard to be implemented involves creation of a new product, service, or marketing channel, must be submitted for approval by the New Products, Services and Channels Committee managed by the Compliance Department.

Roles and responsibilities of the areas in the application/implementation of Cross Regulations

- **Business area responsible for implementation or Product Owner**. Will receive the standard to apply/implement through the regulatory alert system or from the Compliance Department and will convene the Processes Department to analyze which processes are modified or created by the new standard and jointly define the creation of an interdisciplinary team for its implementation. Must budget within 48 business hours for any request of a regulatory nature and ensure the necessary resources for its implementation.
- **Process Department.** Will convene an interdisciplinary team for the implementation of regulations. The team must have at least participation of Legal, Compliance, Internal Control, Risks, the Person in Charge of Protection of Users of Financial Services, Information Technology, Cybersecurity, and any other area deemed necessary.
- **Retail Processes**. Will participate in the analysis and assembly of functional definitions of the process. Develop and modify the corresponding procedure.
- **Compliance Department.** Will analyze and identify regulations that, due to their characteristics, correspond to the "Cross Regulation" category. May request the Process Department to organize a PMO to monitor application/implementation of the standard. Will monitor implementation of standards and issue a monthly report with its status.
- **Legal Advice Department.** Will participate in follow-up meetings providing legal advice for the business.
- **Corporate Department.** At the request of the Process Department, Business Legal Advice or Compliance, must designate a responsible leader to manage implementation of a regulation identified as "Cross Regulation."
- **Responsible Leader.** By designation of the Corporate Manager, must carry out the management of the application/implementation of a "Cross Regulation" together with the Processes Department. Includes interpretation of all aspects related to regulations, obtaining the necessary definitions, completing the application of requirements to the Demand Management area, follow up on the order and its development, participate in project follow-up meetings until final implementation and post-implementation follow-up.
- **Responsible for User Protection of Financial Services.** Will participate in follow-up meetings called by the Processes Department. If necessary, will report on the progress at the request of the external control entity and finally on its application/implementation.
- **Information Technology Department.** As a priority, will assign the necessary resources to complete in a timely manner any request related to regulatory implementation in cases in which an PO is not involved (understanding that when an PO is involved, it is he who defines said assignments).

Rules that regulate internal activities of the bank as a financial entity or in its performance as ALYC

When regulations are not considered "cross," implementation will be responsibility of the sector to which it applies. These types of rules regulate the actions of Grupo Supervielle companies and must be known and implemented by the support areas.

The first line of defense will implement regulations related to products, services, and channels and those that involve the relationship with the client and the support areas will be in charge of implementing those that apply to their specific sectors.

Regulatory Managers. Implementation matrix and normative interpretation.

The persons responsible for application/implementation of regulations by BCRA Ordered Text or specific subject are defined below:

Regulated topics	**Responsible area for implementation**
Labor Relations	HR
Physical security	Operations - Security
Cybersecurity	Risks – Cybersecurity, Cybersecurity COE
Anti-Money Laundering and Financing of Terrorism	Legal
Protection of Financial Services Users	Compliance- Legal - RUSF - DRSF
Foreign trade	Operations - Comex
Foreign exchange	PO that applies
Liquidity and Solvency	Finance
Corporate Governance	Legal - Compliance
Aspects related to Audit	Audit
Information Regimes	Accounting – PO that applies
Risks	Risks
Products	PO that applies
Credit Management, debtor classification	Risks - Credits
Communication by electronic means for the care of the environment	Legal – Compliance - Communications - COE Digital Marketing
Market discipline and minimum disclosure requirements	Risks
Valid identification documents	Legal - AML
Expansion of financial entities	Compliance- Legal
Own portfolio transactions	Finance
Accounting topics	Accounting
Tax Issues	Taxes

Large exposures to credit risk	Risks - Compliance
Financial institutions hours	Legal
Instrumentation, conservation, and reproduction of documents	Operations
Financing to Mipyme	Credits
Guidelines for response and recovery from cyber incidents (RRCI)	Cybersecurity – Cybersecurity COE
Loan origination and management	Credits
Internal controls	Accounting - Internal Control
Social Security Benefit Payments	Business
Net global foreign currency position	Finance
Payment service providers	PO that applies
Non-financial credit providers	Compliance - Legal
Minimum requirements for management, implementation and control of risks related to information technology, information systems and associated resources for financial institutions	Technology – Business – Channels - Technological Risks - Business Continuity Information Security
Complementary services of financial activity and permitted activities	Legal
Financial services in the context of the health emergency	Business - Legal - Compliance
National payment system (immediate debits, direct debits, electronic means of payment, payment services, transfers)	PO that applies
Mutual Guarantee Societies	PO that applies
Consolidated Supervision	Accounting
Securities Conveyor	Operations - Security

Reporting to Compliance Department

Employees leading a development for application/implementation of a particular standard must report to the Compliance Department on a monthly basis progress status of implementations. The Compliance Department may request that information related to the application / implementation of a standard be sent to that Department with a different frequency (weekly, biweekly, etc.)

If standards are in force and have not been able to be applied/implemented, the responsible area will report the action plan for their implementation with defined dates. This information will be incorporated into the regulatory monitoring report that the Compliance Department prepares on a monthly basis.

7. INQUIRIES RELATED TO REGULATORY COMPLIANCE

In order to ensure regulatory compliance and in the event of doubts or differences regarding:
(i) application/implementation of a standard or (ii) the person responsible for regulations, the first line of defense may request the Compliance Department advice in relation to which sector or persons are responsible for evacuating regulatory queries. The Compliance Department will centralize regulatory inquiries that arise after doubts or differences of the first line of defense have been evacuated. The Compliance Department will refer the case to the Ethics, Compliance & Corporate Governance Committee for its treatment, in case of doubts about its resolution.

8. COORDINATION AMONG THE THREE LINES OF DEFENSE

Although each of the lines of defense has individual structure, roles, and responsibilities, they should not function as silos. It is good practice for them to share information and coordinate their activities to (i) ensure adequate coverage and effective risk management and (ii) minimize work duplication.

9. SPECIAL CONTROLS

In order to ensure effective internal control framework and regulatory compliance, when appropriate, the second line of defense will require the Internal Control Department to carry out specific controls on certain critical processes to ensure due compliance of current regulations and avoid sanctions by control agencies. The first line of defense may also require such special controls when it considers that the circumstances so warrant.

10. SAFETY TEST

Grupo Supervielle understands that security of transactions, information provided to customers, risks to be assumed, current regulations and agility and simplicity of operations should not be negatively affected.

For this reason, the areas in charge of implementing or modifying internal systems/processes or procedures should ask themselves the following:

A. **Security.** Does security of customer transactions decrease?
B. **Information.** Does it modify information provided to customers?
C. **Risk.** Does risk increase for the client or the bank?
D. **Normative.** Does it breach any internal regulations or procedures of your knowledge?
E. **Complexity.** Does it make the customer's operation more complex?

In case of doubts about affectation of the aforementioned topics, should consult Information Security for item 1, Legal for items 2, 4 and 5, Risks for item 3, Compliance and Processes for item 3.

11. ETHICS & VALUES LINE

Any breach of this Policy may be reported through the Ethics & Values Line:
0800-777-7813
https://eticagruposupervielle.lineaseticas.com/
User: Supervielle
Password: Supervielle