

ASSA ABLOY

**MANUAL FOR SELF-MONITORING AND COMPREHENSIVE RISK MANAGEMENT
SYSTEM FOR MONEY LAUNDERING, FINANCING OF TERRORISM AND
FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION
(ML/FT/FPWMD) (SAGRILIFT in Spanish)**

ASSA ABLOY SAS SAGRILIFT MANUAL

Approved by the ASSA ABLOY Shareholders' Meeting according to
Minute No. 95 of March 30, 2022

Reviewed by: Jose Luis Tovar

Approved by: Eduardo Cárdenas

Reviewed by: Juan Carlos Zarzur

ASSA ABLOY

Table of Contents

INTRODUCTION	4
1. OBJECTIVE	4
2. SCOPE	4
3. TERMS AND DEFINITIONS	4
4. REGULATORY FRAMEWORK	6
4.1. International Norms and Standards	7
4.2. National Standards	7
5. SELF-MONITORING AND COMPREHENSIVE RISK MANAGEMENT POLICY FOR ML/FT/FPWMD	8
5.1. SAGRILIFT Framework Policy	9
5.2. Cash Transactions	9
6. SAGRILIFT'S RESPONSIBILITIES	9
6.1. Shareholders' Meeting	9
6.2. Legal Representative	10
6.3. Compliance Officer and his/her Deputy	11
6.4. Employees	13
6.5. Responsibilities of the Statutory Auditor	13
7. ML/FT/FPWMD STAGES	13
7.1. Identification of Risk Factors:	14
7.2. Measurement	14
7.3. Control	14
7.4. Monitoring	15
8. ML/FT/FPWMD RISK FACTOR SEGMENTATION AND PROFILING	15
8.1. Customer Segmentation	15
8.2. Supplier Segmentation	16
8.3. Employee Segmentation	16
9. SELF-MONITORING OF THE COMPREHENSIVE RISK OF ML/FT/FPWMD	16
9.1. Periodic Monitoring	17

ASSA ABLOY

9.2.	Customer Warning Signs.....	17
9.3.	Transactional Alerts	18
9.4.	Warning Signs Identified in the Accounting Area.....	18
9.5.	Supplier Warning Signs.....	18
9.6.	Employee Warning Signs.....	19
9.7.	Warning signs of members of the Shareholders' Meeting	20
10.	REPORTS	20
10.1.	Compliance Officer Reports.....	20
10.2.	Unusual Transactions Report.....	21
10.3.	Suspicious Transaction Report.....	22
11.	HANDLING OF REQUESTS FOR INFORMATION.....	23
11.1.	Receipt of requests from supervisory bodies and/or UIAF	23
11.2.	Performing analysis.	23
11.3.	Verification of information.....	23
11.4.	Assembling the file	23
11.5.	Response to the requests.....	23
11.6.	Evaluation of the response by the Legal Department.....	24
11.7.	Sending the response to the supervisory body	24
11.8.	Reporting to the General Meeting.....	24
11.9.	Filing of information	24

ASSA ABLOY

INTRODUCTION

ASSA ABLOY Colombia SAS, hereinafter ASSA ABLOY, committed to complying with Colombian regulations, establishes guidelines for the identification, measurement, control and monitoring for the prevention of money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction (ML/FT/FPWMD).

1. OBJECTIVE

This manual is applicable to the entire ASSA ABLOY organization; its objective is to ensure compliance and applicability of the policies and guidelines for the prevention and control of money laundering, financing of terrorism, and proliferation of weapons of mass destruction (ML/FT/FPWMD) through the performance of the Shareholders' Meeting, business partners, employees and any other stakeholders and all counterparties related to the development of the organization, as established by the Superintendency of Companies and company policies.

2. SCOPE

This manual also aims to provide the measures and tools to report internally and externally, when applicable, any faults or noncompliance identified in accordance with the guidelines set forth in the current legislation. In cases of conflict between legislation and ASSA ABLOY's internal procedures, the one that establishes the strictest requirements shall always prevail.

3. TERMS AND DEFINITIONS

- a. **Money Laundering (ML):** Anyone who acquires, safeguards, invests, transports, transforms, stores, conserves, guards or administers assets that have their mediate or immediate origin in activities of migrant smuggling, human trafficking, extortion, illicit enrichment, kidnapping for ransom, rebellion, arms trafficking, trafficking of minors, financing of terrorism and administration of resources related to terrorist activities, trafficking of toxic drugs, narcotics or psychotropic substances, crimes against the financial system, crimes against the public administration, smuggling, smuggling of hydrocarbons or their derivatives, customs fraud or favoring and facilitating smuggling, favoring smuggling of hydrocarbons or their derivatives, in any of its forms, or linked to the proceeds of crimes executed under a criminal conspiracy, or giving the assets derived from such activities the appearance of legality or legalizing, hiding or concealing the true nature, origin, location, destination, movement or right over such assets.

ASSA ABLOY

- b. Financing of Terrorism (FT):** Whoever directly or indirectly provides, collects, delivers, receives, administers, contributes, safeguards, or keeps funds, assets, or resources or performs any other act that promotes, organizes, supports, maintains, finances, or economically sustains organized crime groups, illegal armed groups or their members, or national or foreign terrorist groups, national or foreign terrorists, or terrorist activities.
- c. Financing the Proliferation of Weapons of Mass Destruction (FPWMD):** Is any act that provides funds or uses financial services, in whole or in part, for the manufacture, acquisition, possession, development, export, material transfer, fractionation, transportation, transfer, deposit or dual use for illegitimate purposes in contravention of national laws or international obligations, when the latter is applicable.
- d. ML/FT/FPWMD Risk:** Is the possibility of loss or damage that a Company may suffer due to its propensity to be used directly or through its operations as an instrument for Money Laundering and the channeling of resources towards terrorist activities or the Financing of the Proliferation of Weapons of Mass Destruction, or when the concealment of Assets derived from such activities is intended. The contingencies inherent to ML/FT/FPWMD materialize through risks such as Contagion Risk, Legal Risk, Operational Risk, Reputational Risk, and others to which the Company is exposed, with the consequent negative economic effect that this may represent for its financial stability when it is used for such activities.
- e. ML/FT/FPWMD Risk Factors:** These are the possible elements or causes that generate ML/FT/FPWMD Risk, considering the Counterparties, Products, activities, channels, and jurisdictions, among others.
- f. ML/FT/FPWMD:** Money Laundering, Financing of Terrorism and Financing of the Proliferation of Weapons of Mass Destruction.
- g. Counterparty:** Any natural or legal person with whom the Company has commercial, business, contractual, or legal ties of any kind. For ASSA ABLOY, counterparties are the members of its Shareholders' Meeting, customers, suppliers, and employees.
- h. Due Diligence:** Refers to the periodic review of legal, accounting, and financial aspects related to commercial ties, which aims to identify and assess the risks of money laundering, the financing of terrorism, and the financing of the proliferation of weapons of mass destruction that may affect ASSA ABLOY.
- i. Unusual Transaction:** A transaction whose amount or characteristics are not related to the ordinary or normal economic activity of ASSA ABLOY, which by its number, amount, or characteristics does not fall within the regular patterns or ordinary business practices in a sector, industry, or with a class of Counterparty.

ASSA ABLOY

- j. **Suspicious Transaction:** An Unusual Transaction that, in addition, according to the uses and practices associated with the activity in question, could not be reasonably justified. This type of transaction includes attempted or rejected transactions that contain characteristics that make them suspicious.
- k. **Attempted Transaction:** A financial transaction that a business associate (a natural or legal person) attempts to carry out but is not carried out, the person desists from doing it, or the established controls do not allow it to be carried out.
- l. **Rejected Transaction:** A financial transaction that a business associate (a natural or legal person) carries out but is rejected or the established controls do not allow it to be carried out.
- m. **STR:** It is the Suspicious Transactions report. It is a transaction that, due to its number, amount, or characteristics, does not fall within the normal system and practices of the business of a particular industry or sector and, besides, according to the uses and practices of the activity in question, could not be reasonably justified.
- n. **PEP (Politically Exposed Person):** These are public servants of any nomenclature and job classification system of the national and territorial public administration when, in the positions they hold, they have as part of the duties of the area to which they belong or in those of the employment record they occupy, under their direct responsibility or by delegation, the general direction of formulation of institutional policies and adoption of plans, programs, and projects and the direct management of assets, money or securities of the state. These may be through expenditure management, procurement, management of investment projects, payments, settlements, and movable and immovable property administration. It also includes Foreign PEPs and PEPs of International Organizations.
- o. **PEPs of International Organizations:** These refer to natural persons who perform managerial functions in an international organization, such as the United Nations, the Organization for Economic Cooperation and Development, the United Nations International Children's Emergency Fund (UNICEF), and the Organization of American States, among others (e.g., directors, deputy directors, members of the Shareholders' Meeting or any person who performs an equivalent function).
- p. **Foreign PEPs:** These are natural persons who perform prominent and outstanding public functions in another country. In particular, the following persons: heads of state, politicians, high-ranking government, judicial or military officials, and senior executives of state-owned enterprises.

4. REGULATORY FRAMEWORK

4.1. International Norms and Standards

This manual complies with the following international norms in force regarding the prevention of money laundering, the financing of terrorism, and the financing of the proliferation of weapons of mass destruction (ML/FT/FPWMD); therefore, this manual is derived from the following norms:

- a) 1988 Vienna Convention: United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Approved by Law 67 of 1993 - Sentence C-176 of 1994).
- b) United Nations Convention for the Suppression of the Financing of Terrorism of 1999 (Approved by Law 808 of 2003 - Sentence C-037 of 2004).
- c) Palermo Convention of 2000: United Nations Convention Against Transnational Organized Crime (Approved by Law 800 of 2003 - Sentence C-962 of 2003).
- d) Mérida Convention of 2003: United Nations Convention Against Corruption (Approved by Law 970 of 2005 - Sentence C-172 of 2006).
- e) Recommendations of the Financial Action Task Force (FATF) that include a set of standards designed to provide a comprehensive plan against money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction.

4.2. National Standards

This Manual complies with the Colombian legislation in force regarding the prevention of money laundering, the financing of terrorism, and the financing of the proliferation of weapons of mass destruction (ML/FT/FPWMD); therefore, this Manual is derived from the following norms:

- a) Circular 100-000016 of December 24, 2020 – Comprehensive Amendment to Chapter X of the Basic Legal Circular of 2017.
- b) Law 526 of 1999 – Creation of the Financial Information and Analysis Unit (UIAF in Spanish)

Regarding the prevention of money laundering, the financing of terrorism, and the financing of the proliferation of weapons of mass destruction (ML/FT/FPWMD), with respect to the activity developed by ASSA ABLOY as a Customs User, apart from the legislation mentioned in the previous paragraph, the following regulations are complied with:

ASSA ABLOY

- a) External Circular 170 of 2002 DIAN (the National Directorate of Taxes and Customs in Colombia) – Prevention and Control of Money Laundering.
- b) Resolution 285 of 2007 UIAF– Obligation to report directly to the UIAF.
- c) Resolution 212 of 2009 UIAF – Addendum to Resolution 285 of 2007.
- d) Resolution 017 of 2016 UIAF – Amendment to Resolution 212 of 2009.

5. SELF-MONITORING AND COMPREHENSIVE RISK MANAGEMENT POLICY FOR ML/FT/FPWMD

This Policy is designed to mitigate the materialization of risks of money laundering, financing of terrorism, and financing of the proliferation of weapons of mass destruction, providing the rules for compliance with all national and international laws and regulations implemented in the fight against these crimes.

Therefore, for the implementation of this Manual, other policies and procedures related to it, the following guidelines are determined:

- a) The Shareholders' Meeting, Managers, and employees must be verified by validating matches in binding lists, conducting background checks, and updating data regularly. If a "Positive" report is found, ASSA ABLOY will refrain from continuing the employment or contractual relationship with the employee.
- b) The Shareholders' Meeting, Managers, clients, suppliers, and employees are committed to the prevention of ML/FT/FPWMD; therefore, their duty is to comply with the policies and procedures established when, due to the nature of their functions, they need to execute operations, businesses or enter into contracts, ensuring their veracity and legality.
- c) Prior to their performance, customers and suppliers are subject to strict verifications before and after the formalization of the commercial relationship, either through contracts, acceptance of service proposals, and/or acceptance of service or purchase orders, in order to comply with the due diligence within the legal regulatory framework and with the procedures for selection and knowledge of customers and suppliers. ASSA ABLOY will therefore refrain from entering into relationships with legal entities or individuals on binding lists.
- d) ASSA ABLOY will carefully analyze those who appear on informative lists (non-restrictive) due to processes that link them to criminal activities or activities associated with ML/FT/FPWMD and that may affect the company's reputation, and will refrain from hiring them or continuing the commercial relationship.
- e) Any commercial, employment, or legal relationship will be terminated with natural or legal persons who, during the development of contractual activities and through due diligence, are found to have carried out suspicious operations.

5.1. SAGRILIFT Framework Policy

ASSA ABLOY complies with the Colombian regulations that support SAGRILIFT through the application of the parameters established in this Manual, the guidelines of Self-Monitoring and Comprehensive Risk Management Policy for ML/FT/FPWMD, and the Code of Conduct for its employees and third parties.

Therefore, the SAGRILIFT system will be disclosed to the Shareholders' Meeting, customers, suppliers, employees, and all those who are involved in the economic activity to the extent required. Additionally, training will be provided to employees who are deemed to be familiar with the system to ensure that they are able to report any unusual operation they identify as part of the activities inherent to their position.

5.2. Cash Transactions

ASSA ABLOY has determined that cash transactions only occur in the following cases:

5.2.1. Income

- **Showroom sales**, which must be managed in accordance with the procedure established for such purpose and in the following amounts:
 1. Cash receipts of less than \$9,990,000 will be allowed.
 2. For amounts between \$6,000,000 and \$9,990,000, the signature of the **Form of Knowledge - Origin of Funds - Authorization to Consult and Send Information** must be requested and the provisions of the SAGRILIFT Procedures Manual regarding customer due diligence must be applied.

5.2.2. Output:

- **Pretty Cash Management**, which is authorized by the Financial Manager and administered by the Head of Treasury and Portfolio in accordance with the company's internal procedures.

6. SAGRILIFT'S RESPONSIBILITIES

6.1. Shareholders' Meeting

- a) Approve the Policy for the prevention and control of the risk of money laundering, the financing of terrorism, and the financing of the proliferation of weapons of mass destruction ML/FT/FPWMD.
- b) Approve this SAGRILIFT Manual and its updates, submitted by the legal representative and the Compliance Officer.

ASSA ABLOY

- c) Order the technical and human resources required to implement and maintain SAGRILIFT in operation.
- d) Appoint the Compliance Officer and his/her Deputy.
- e) Include in the agenda of its meetings the presentation of the Compliance Officer's, his/her Deputy's, and/or Statutory Auditor's report when the latter deems it necessary.
- f) Timely analyze the reports on the operation of SAGRILIFT, the proposals for corrective measures, and the updates submitted by the Compliance Officer or his/her Deputy and make decisions regarding all the topics discussed. This shall be recorded in the minutes of the corresponding meetings.
- g) Comment on the reports submitted by the Statutory Auditor's Office related to the implementation and operation of SAGRILIFT and carefully review the remarks or recommendations included. This review and the periodic improvements shall be recorded in the corresponding minutes.
- h) Order and guarantee the technical, logistical, and human resources necessary to implement and maintain SAGRILIFT in operation, according to the requirements of the Compliance Officer or his/her Deputy.
- i) Verify that the Compliance Officer or his/her Deputy has the necessary availability and capacity to perform his/her duties.
- j) Verify that ASSA ABLOY, the Compliance Officer, and the legal representative carry out the activities designated in this Chapter X and in SAGRILIFT.

6.2. Legal Representative

- a) Submit with the Compliance Officer or his/her Deputy, for approval of the Shareholders' Meeting, the proposal of SAGRILIFT and its updates.
- a. Study the results of the ML/FT/FPWMD Risk assessment carried out by the Compliance Officer or his/her Deputy and establish the corresponding action plans.
- b) Efficiently allocate the technical and human resources, as determined by the Shareholders' Meeting, necessary to implement the SAGRILIFT.
- c) Verify that the Compliance Officer or his/her Deputy has the necessary availability and capacity to perform his/her duties.

ASSA ABLOY

- d) Provide effective, efficient, and timely support to the Compliance Officer or his/her Deputy in the design, management, supervision, and monitoring of SAGRILAFT.
- e) Submit to the Shareholders' Meeting the reports, requests, and alerts it considers should be addressed and that are related to SAGRILAFT.
- f) Ensure that the activities resulting from the development of SAGRILAFT are duly documented so that the information meets the criteria of integrity, reliability, availability, compliance, effectiveness, efficiency, and confidentiality.
- g) Verify that SAGRILAFT procedures comply with the ML/FT/FPWMD Policy adopted by the Shareholders' Meeting.

6.3. Compliance Officer and his/her Deputy

The ASSA ABLOY Shareholders' Meeting shall appoint the Compliance Officer or his/her Deputy, who shall be internally responsible for the prevention of money laundering, the financing of terrorism, and the financing of the proliferation of weapons of mass destruction (ML/FT/FPWMD), based on the following duties:

- a) Ensure effective, efficient, and timely compliance with SAGRILAFT.
- b) Submit reports to the Shareholders' Meeting, or failing that, to the highest corporate body, which shall contain an assessment and analysis of the efficiency and effectiveness of SAGRILAFT and, if necessary, propose the respective improvements. Likewise, demonstrate the results of the management of the Compliance Officer or his/her Deputy and the Company's management in general in complying with SAGRILAFT.
- c) Promote the adoption of corrective measures and updates to SAGRILAFT when circumstances so require.
- d) Verify the timely and strict compliance with the legal norms established to prevent criminal activities in international trade.
- e) Implement the general and specific procedures it deems appropriate to make this work more effective.
- f) Periodically monitor and verify the implementation of the measures adopted in this field and the information provided by ASSA ABLOY's active customers and suppliers.

ASSA ABLOY

- g) Conduct the necessary studies to determine whether an unusual transaction in foreign trade transactions is suspicious.
- h) Inform the ASSA ABLOY Shareholders' Meeting about possible failures or omissions in the controls to prevent criminal activities, which compromise the responsibility of employees and the company.
- i) Submit a detailed monthly report on the fulfillment of the tasks under his/her responsibility to the Legal Representative.
- j) Propose the necessary adjustments or modifications to SAGRILIFT's policies to the Shareholders' Meeting.
- k) Design, program, and coordinate the necessary training plans on the subject so that the different employees of the organization are duly informed and updated.
- l) Identify situations that may create a risk of money laundering, financing of terrorism, and financing of the proliferation of weapons of mass destruction (ML/FT/FPWMD) in the operations carried out by the organization.
- m) Verify the adoption and operation of the procedures defined for the adequate management, conservation, and storage of records and reports related to the prevention of the risk of money laundering, financing of terrorism, and financing of the proliferation of weapons of mass destruction (ML/FT/FPWMD).
- n) Prepare the reports and update the database registered in the SIREL Online Reporting System.
- o) Receive and analyze internal reports of possible unusual, attempted, or suspicious transactions and prepare a report in accordance with the applicable legal requirements.
- p) Handle and coordinate any requirement, request, or proceeding from judicial or administrative authorities regarding the prevention and control of criminal activities.
- q) Report suspicious transactions to the Financial Information and Analysis Unit (UIAF).
- r) Maintain updated internal documents containing policies and procedures through SAGRILIFT.

6.4. Employees

All ASSA ABLOY employees, regardless of their position, hierarchy, duties, and roles, must comply with the following functions as part of their responsibilities with the Self-Monitoring and Comprehensive Risk Management System for ML/FT/FPWMD.

- a) Attend trainings designated by the organization related to the prevention of the risk of money laundering, financing of terrorism, and financing of the proliferation of weapons of mass destruction (ML/FT/FPWMD).
- b) Report to the Compliance Officer unusual operations related to the warning signs in the departments exposed to the risk of money laundering, financing of terrorism, and financing of the proliferation of weapons of mass destruction (ML/FT/FPWMD).

6.5. Responsibilities of the Statutory Auditor

The Statutory Auditor must include in his/her audit plan the programs to verify compliance with the prevention, control, and detection of money laundering, financing of terrorism, and financing of the proliferation of weapons of mass destruction (ML/FT/FPWMD), in accordance with the legal regulations in force and the procedures established by the organization.

Likewise, it must verify the operations, businesses, and contracts entered into or fulfilled by the company in accordance with the instructions given by the Shareholders' Meeting, such as:

- a) Customer transactions
- b) Transactions with suppliers
- c) Financial transactions of the Shareholders' Meeting

The Statutory Auditor is responsible for reporting any new developments to the Compliance Officer regarding the financial red flags identified.

7. ML/FT/FPWMD STAGES

ASSA ABLOY establishes the following stages for the implementation of controls focused on the prevention of ML/FT/FPWMD:

7.1. Identification of Risk Factors:

Based on the nature of ASSA ABLOY's operations, the following risk factors have been determined for the company through which segmentation will be applied in order to implement differentiated monitoring strategies for counterparties according to the combination of each ML/FT/FPWMD risk factor and other variables:

- a) **Suppliers:** Those who provide services or products for the company's functioning and operation.
- b) **Customers:** Those who purchase ASSA ABLOY's products.
- c) **Officers:** The company's direct employees, who are considered essential counterparts to apply due diligence to prevent ML/FT/FPWMD risks.
- d) **Shareholders' Meeting:** The individuals or legal entities that invested their own resources to capitalize the company.

7.2. Measurement

Each risk factor is measured by identifying potential illicit activities that could occur. These measurements are composed of a previous definition of the risk context and risk factor, through which the inherent risk is measured under the concepts of impact (loss) and frequency or probability of occurrence of the event with the scales and parameters that have been established in the **Risk Management Procedure**. This methodology must be applied to all risk factors, as well as when entering new markets or offering new lines of business.

7.3. Control

After measuring the inherent risk according to each factor, the existing controls that the company has adopted to prevent or detect inherent risk events are determined, and the control is evaluated according to its effectiveness and application to subsequently estimate the residual risk, through which it is determined whether it is necessary to apply new controls to reduce the probability or impact of the risks determined by ASSA ABLOY, supported in the **International Supply Chain Risk Identification and Management Matrix**.

ASSA ABLOY guarantees the means of reporting unusual transactions (internally) and suspicious transactions to the UIAF, as it has provided the following channels:

- a) Internal reporting channels: any unusual activity should be reported by employees to the local Compliance Officer.

- e) External reporting channels: in case of any illicit or suspicious activity associated with ML/FT/FPWMD, report suspicious transactions immediately to the UIAF with the nature of “STR” (Suspicious Transaction Report) through the Online Reporting System (SIREL in Spanish).

7.4. Monitoring

ASSA ABLOY monitors annually or when additional red flags are identified, reviewing the **International Supply Chain Risk Identification and Management Matrix** and verifying compliance with the proposed controls.

The Compliance Officer must verify that the controls that have been formulated are being implemented promptly in accordance with the dates established in the document and that they are effective, i.e., that their implementation contributes to risk mitigation and favors the company. If the Compliance Officer identifies that these controls are not effective, efficient, or timely, he/she must perform a new analysis, involve the process leaders he/she considers pertinent, redefine the controls, define new dates for monitoring and verification, and leave evidence of these activities in the form of meeting minutes.

8. ML/FT/FPWMD RISK FACTOR SEGMENTATION AND PROFILING

ASSA ABLOY has established procedures and activities required to segment the risk factors of Money Laundering, Financing of Terrorism, and Financing of the Proliferation of Weapons of Mass Destruction (ML/FT/FPWMD) in order to identify those segments that require a more detailed level of monitoring.

8.1. Customer Segmentation

ASSA ABLOY has the **ANX.019 Portfolio Policy** that describes Due Diligence, and the verification is performed based on multiple attributes (e.g., chamber of commerce, Single Tax Registry in Colombia - RUT, verification on restrictive lists including partners, shareholders, and boards of directors). This data is included in the **FOR.065 Customer Relationship Form** with their respective agreements. In addition, the **SAGRILIFT and Transparency and Business Ethics Program (PTEE in Spanish) Procedures Manual** has been established, where the segmentation methodology is determined.

It should be clarified that if the customer is on non-binding lists, is a PEP (Politically Exposed Person), has an activity sensitive to money laundering, financing of terrorism, and financing of proliferation of weapons of mass destruction, or carries out the activity in higher-risk countries, it will be classified as high risk, and the

ASSA ABLOY

Compliance Officer will be immediately notified for its respective control and monitoring.

Based on the evaluation made through the due diligence process for third parties, the need for a customer visit will be defined. When a customer is classified as high-risk, a visit for customer knowledge will be necessary prior to the authorization to enter into a business relationship with the customer. During such visit, the “**Form of Security Visit to Customers**,” designed to determine the suitability of the third party in a more exhaustive way, shall be filled in and proceed as indicated therein.

8.2. Supplier Segmentation

For supplier profiling, ASSA ABLOY has a **Supplier Management Procedure PRO.018**, which determines the parameters to be followed for the selection, evaluation, and knowledge of suppliers to ensure their reliability. The Procurement process is responsible for verifying the binding and restrictive lists, including partners, shareholders, and boards of directors, related to the documentation delivered (chamber of commerce, RUT, etc.), before its creation in the system. The information in the selection process is applied as contemplated in the **SAGRILIFT and PTEE Procedures Manual**, where the methodology for segmentation is determined.

Suppliers who are on non-binding lists, who are PEPs (Politically Exposed Persons), have an activity that is sensitive to money laundering, terrorist financing, and financing of the proliferation of weapons of mass destruction, or carry out the activity in higher-risk countries, will be classified as high-risk, and the Compliance Officer will be immediately notified for their respective control and monitoring.

8.3. Employee Segmentation

ASSA ABLOY has determined within its controls the employees' profiles through the **Job Description** and its relationship according to **PRO.021 Personnel Selection Procedure (Direct and Temporary)**, in which guidelines have been established to manage the knowledge, evaluation, and selection of personnel who perform activities that affect the quality of services offered to ASSA ABLOY. In addition, the **SAGRILIFT and PTEE Procedures Manual** has established the methodology for personnel segmentation to identify those at high risk and thus determine the type of due diligence to be applied.

9. SELF-MONITORING OF THE COMPREHENSIVE RISK OF ML/FT/FPWMD

ASSA ABLOY

ASSA ABLOY has determined through the Supplier Management Procedure, Personnel Selection Procedure, and Portfolio Policy the due diligence of knowledge and updating of its Customers, Suppliers, and Employees.

9.1. Periodic Monitoring

ASSA ABLOY has determined that controls for any business partners and employees should be applied prior to joining and annually thereafter through verification on binding and restrictive lists by a specialized provider, updating of data, and documents of counterparties to ensure that they do not present any news or negative reports.

9.2. Customer Warning Signs

The following are the warning signs to be considered with Customers to mitigate the risks of money laundering, financing of terrorism, and proliferation of weapons of mass destruction (ML/FT/FPWMD) in ASSA ABLOY:

- a) The Customer refuses to provide the requested information, or the information provided is inconsistent or difficult for ASSA ABLOY to verify.
- b) The Customer indicates an address that is also the address of a business other than the one declared by the customer and/or does not seem to correspond to the occupation stated by the customer (e.g., student, unemployed, self-employed).
- c) The Customer requests to be excluded from the requested requirements.
- d) The Customer refuses to fill out the forms required by the company or to provide the information necessary to complete them or to carry out the transaction once the Customer is requested to fill out the forms.
- e) The Customer frequently uses intermediaries to carry out commercial or financial transactions.
- f) Financial transactions do not correspond to the Customer's profile.
- g) The financial statements submitted by the Customer reveal a financial situation that differs from that of similar businesses.
- h) The Customer insists on meeting the Company's personnel at a location other than the offices to carry out a transaction.
- i) The Customer attempts to pressure an ASSA ABLOY employee not to fill out the forms required by ASSA ABLOY.

ASSA ABLOY

- j) It becomes known through the public media or otherwise, as applicable, that a Customer is being investigated or prosecuted for the offense of money laundering, predicate offenses, terrorism financing, and the proliferation of weapons of mass destruction.
- k) The Customer repeatedly performs fractional transactions.
- l) The Customer constantly performs transactions and unusually uses or intends to use cash as the only means of payment instead of other means.

9.3. Transactional Alerts

The following are the transactional warning signs to be considered in mitigating the risks of money laundering, financing of terrorism, and proliferation of weapons of mass destruction (ML/FT/FPWMD) in ASSA ABLOY:

- a) The Customer shows growth in assets, equity, and income more than twice or more compared to the sector.
- b) The Customer makes an advance payment for a product or service and then requests a money return regularly and/or for large amounts.

9.4. Warning Signs Identified in the Accounting Area

- a) Loss of certain accounting records.
- b) Identify annual operations in amounts of transactions and transfers to customers.
- c) Incorrect entries in the company's accounts for subsequent reimbursement to accounts not registered by customers or any other type of natural or legal person.
- d) Alerts generated in the statutory audit reports.

9.5. Supplier Warning Signs

The following are the warning signs to be considered with suppliers to mitigate the risks of money laundering, financing of terrorism, and proliferation of weapons of mass destruction (ML/FT/FPWMD) in ASSA ABLOY:

- a) Suppliers are unwilling to provide information requested by ASSA ABLOY in the linking or upgrading process.
- b) Change of supplier owners with a history inconsistent with the nature of the business.

ASSA ABLOY

- c) Limited, false, or suspicious information provided by the supplier
- d) Unusual activities in the context of the supplier's business.
- e) Industries or economic activities of the supplier that are inherent to the risk of money laundering, financing of terrorism and proliferation of weapons of mass destruction.
- f) Threat or attempt to bribe any employee to accept incomplete or false information and/or want to enter into a relationship without complying with the procedures for supplier relationships.
- g) Suppliers that, after their linking, are included in the binding lists related to money laundering, financing of terrorism, and proliferation of weapons of mass destruction.
- h) Transactions that are frequently carried out in the name of third parties without any justification for doing so.
- i) Suppliers seeking to establish business relationships with ASSA ABLOY without references.

9.6. Employee Warning Signs

The following are the warning signs to be considered with employees to mitigate the risks of money laundering, financing of terrorism, and proliferation of weapons of mass destruction (ML/FT/FPWMD) in ASSA ABLOY:

- a) The employee's lifestyle does not correspond to their income, or there is a noticeable and unexpected change in their economic situation.
- b) The employee has frequent and unjustified absences.
- c) The employee uses their home address to receive company documents.
- d) The employee has or insists on having meetings with the company's customers through non-corporate virtual channels or in places other than the company's offices, as well as outside working hours, without any justification whatsoever to carry out a commercial or financial operation.
- e) The employee shows an unusual or sudden growth in the number of operations under their responsibility.

ASSA ABLOY

- f) It is verified that the employee has not reported or has concealed information to the compliance officer regarding the change in the behavior of a customer or supplier.
- g) The employee receives gifts, invitations, and benefits from certain customers or counterparties without a clear and reasonable justification.
- h) The employee exempts a customer or supplier from controls with the argument that they are "associates that they know completely."
- i) The employee constantly changes its address and/or telephone number.
- j) The employee is reluctant to go on vacation and has accumulated more than two periods.

9.7. Warning signs of members of the Shareholders' Meeting

The following are the warning signs to be considered with the members of the Shareholders' Meeting to mitigate the risks of money laundering, financing of terrorism, and proliferation of weapons of mass destruction (ML/FT/FPWMD) in ASSA ABLOY:

- a) Refusing to update information when required to do so.
- b) When there are matches in the identification number or name when validating it in binding or restrictive lists or other sources.
- c) Identifying assets related to offenses associated with money laundering, financing of terrorism, and the proliferation of weapons of mass destruction intended to be received as contributions from associates.
- d) The impossibility of identifying the origin of the contributions made by the shareholder.

10. REPORTS

10.1. Compliance Officer Reports

The Compliance Officer shall submit periodic reports to the Shareholders' Meeting. This must mention the evaluation and analysis of the efficiency and effectiveness of SAGRILIFT and, if applicable, the respective improvements. This report may contain, among others:

- a) Progress in the implementation of the policies and procedures contained in the

SAGRILIFT Manual.

- b) New ML/FT/FPWMD risks identified.
- c) Record of unusual operations reported and the results of the analysis performed.
- d) Progress in the development of outreach and training plans designed.
- e) Action plans implemented in response to the remarks made by the ASSA ABLOY Shareholders' Meeting in the event of any pronouncements made by this body.
- f) Possible failures or omissions in controls for the prevention and control of money laundering, financing of terrorism, and proliferation of weapons of mass destruction.
- g) Response to requirements and recommendations of the Shareholders' Meeting and submission of reports to control and oversight bodies.

10.2. Unusual Transactions Report

If, as part of the activities under their responsibility, an employee detects an unusual transaction based on the warning signs mentioned in this manual, the employee must report it to the immediate supervisor. The immediate supervisor shall send an email to the Compliance Officer with the Subject: Unusual Transaction Report and shall attach the Internal Suspicious Transaction Report form, which includes:

- Report date and date of the unusual transaction
- Name and Surname of the reporting employee
- Type of related counterparty
- Name and identification number of the related counterparty
- The warning sign detected
- Clear reasons for which the transaction is considered unusual
- Any additional information you deem relevant

If a month goes by without an unusual transaction, the Compliance Officer shall send an email to the process leaders to confirm whether there was indeed no unusual activity. If, after three business days, the leaders do not report any unusual transactions, this shall be the Compliance Officer's evidence to report the absence of a suspicious transaction to the UIAF.

All employees are obliged to keep the unusual transaction report confidential.

10.3. Suspicious Transaction Report

Based on the unusual transaction reported, the Compliance Officer shall analyze the information and, if deemed necessary, may request additional data and documentation from ASSA ABLOY's areas so that they may request it from customers and counterparties.

Some objective criteria have been established for the Compliance Officer to determine whether it is a suspicious transaction.

- a) Positive or exact matches during the consultation in the lists.
- b) The value of the transaction, contract, or negotiation is inconsistent with the financial capacity of the counterparty, economic activity, or corporate purpose and has no reasonable justification.
- c) The counterparty's funds are presumed to be of illicit origin.
- d) The financial behavior of the counterparty is atypical in relation to the information on the economic variables of the market segment to which its activity corresponds.
- e) Pretending to enter into a contractual agreement without complying with the legal and internal requirements.
- f) If there is reasonable doubt that the information provided by the counterparty is false or misleading, seeking to conceal issues of money laundering, financing of terrorism, and/or financing of the proliferation of weapons of mass destruction.
- g) The reason for the unusuality cannot be identified.
- h) Any other situation that the Compliance Officer considers suspicious.

The Compliance Officer shall report suspicious transactions immediately as "STRs" to the UIAF through the Online Reporting System (SIREL).

The filing of an STR does not constitute a criminal complaint. Therefore, for reporting purposes, the company does not need to be sure that it is a criminal activity, nor is it required to identify the criminal offense or verify that the resources have an illicit origin. However, since it is not a criminal complaint, it does not exempt the company or its administrators from the obligation to report where applicable.

ASSA ABLOY

In the event that a quarter passes without the company making an STR, the Compliance Officer, within ten (10) calendar days following the expiration of the respective quarter, must submit through SIREL, and with the nature of "AROS," the absence of a suspicious transaction in accordance with the calendar defined by the UIAF.

Once the Compliance Officer receives the UIAF's consecutive receipt number, the Compliance Officer shall print it and keep it in the file with the STR or AROS supporting documents.

It is the Compliance Officer's responsibility to keep the documents that support the decision to determine a transaction as suspicious in order to provide them in a complete and timely manner to the authorities when they request them.

11. HANDLING OF REQUESTS FOR INFORMATION

Requests for information from competent authorities shall be handled by the Compliance Officer as follows:

11.1. Receipt of requests from supervisory bodies and/or UIAF

Once a request is received from the supervisory bodies and/or UIAF, it must be delivered to the Compliance Officer, who in turn shall inform the Legal Representative, the Shareholders' Meeting, and the Statutory Auditor of the receipt of the request as required.

11.2. Performing analysis.

The Compliance Officer shall analyze the request sent by the supervisory body and/or UIAF, requesting the information associated with the request from the corresponding person (area, employee, etc.).

11.3. Verification of information.

The Compliance Officer shall verify that the information provided is reliable and serves as evidence to respond to the body that requires it.

11.4. Assembling the file

With the information obtained, the Compliance Officer shall assemble a folder where the file is filed chronologically.

11.5. Response to the requests

The file is used to analyze the request from the supervisory body and/or UIAF and an initial response to the request is drafted.

11.6. Evaluation of the response by the Legal Department

The initial response to the request shall be sent to the Legal Department for review and approval.

11.7. Sending the response to the supervisory body

Once the Legal Department has approved the response, it shall be signed by the Legal Representative for subsequent submission to the supervisory body and/or UIAF, including the respective supporting documents.

11.8. Reporting to the General Meeting

In its periodic report, the Compliance Officer shall update the General Meeting on the status of the receipt/sending of responses to requests from supervisory bodies and/or UIAF.

11.9. Filing of information

The Compliance Officer shall file the information along with the supporting documents sent.

12. DOCUMENT PRESERVATION

The SAGRILAFT documentation includes the SAGRILAFT Manual, Procedures Manual, procedures, know-your-counterparty forms, documents provided by the counterparties, Compliance Officer reports, ML/FT/FPWMD risk matrix, documentation of dissemination and training, requests for information by competent authorities with their responses, unusual transaction reports with their supporting documents, suspicious transaction reports with their supporting documents, reports of the absence of a suspicious transaction, among others.

Those responsible within ASSA ABLOY for the SAGRILAFT documentation shall ensure its integrity, reliability, availability, compliance, and confidentiality. Likewise, due diligence records shall be kept for at least six years; if the counterparty has left the company, the last due diligence renewal shall be kept for the following six years.

13. INDICATORS

TYPE OF INDICATOR	PERSON RESPONSIBLE FOR THE MEASUREMENT	FORMULA	GOAL	PERIODICITY
Efficiency	Compliance Officer	Total number of people trained in SAGRILAFT / Total ASSA ABLOY employees	> 95%	Annual
Informative	Compliance Officer	Total unusual transactions reported	< 5	Annual

ASSA ABLOY

Effectiveness	Compliance Officer	Total suspicious transactions	0	Annual
Efficiency	Human Resources	Number of high-risk employees with intensified due diligence per day/ Number of high-risk employees	100%	Semiannual
Efficiency	Commercial and Portfolio	Number of high-risk customers with intensified due diligence per day/ Number of high-risk customers	100%	Semiannual
Efficiency	Purchases	Number of high-risk suppliers with intensified due diligence per day/ Number of high-risk suppliers	100%	Semiannual
Efficiency	Board of Directors	Number of high-risk partners or shareholders with intensified due diligence per day/ Number of high-risk partners or shareholders	100%	Semiannual
Efficiency	Compliance Officer and Counterparty Manager	Number of information pieces in PTEE and SAGRILIFT	≥ 6	Annual