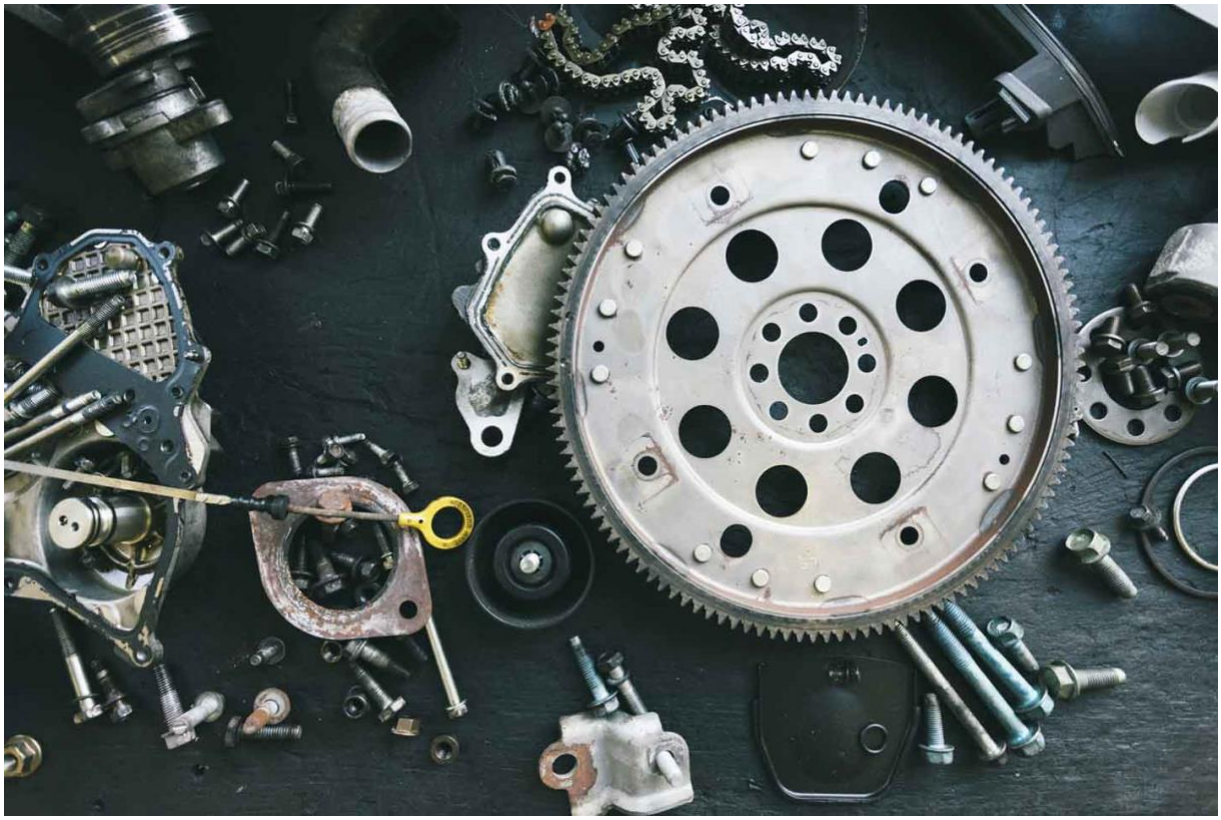
Service de Renseignement Financier
(Financial Intelligence Unit)

REPOBLIKAN'I MADAGASIKARA
Fitiavana–Tanindrazana – Fandrosoana

SAMIFIN
AU SERVICE DE L'ECONOMIE

DNFBP'S RISK BASED SUPERVISION MANUAL

OCTOBER 2025



CONTENT

Preamble ***3***

Important Terms 3
Who is Controlled and Where? 3
Basic Principles of Supervision 3
What the Manual Will Describe 4

Part I – Introduction ***4***

1.1 What is the purpose of this manual? 4
1.2 Principles Guiding Supervision 4
1.3 Governance of the Manual 5

Part II – Laws and Institutions **5**

2.1 Main Laws 5
2.2 Who Does What Nationally? 6
2.3 International Cooperation 6

Part III – Risk-Based Supervision Model **7**

3.1 The Three Key Ideas of Risk 7
3.2 How is Risk Simply Calculated? 7
3.3 Minimum Data to be Provided 9
3.4 Application of the Risk-Based Approach 9

Part IV – Off-site Supervision **11**

4.1 What is the purpose of off-site control? 11
4.2 The Off-site Questionnaire 11
4.3 Document Verification 11
4.4 Indicators and Alert Levels 12
4.5 Analysis, Dialogue, and Follow-up 12

Part V – Targeted Financial Sanctions (TFS) and CNSFC **12**

5.1 From Designation to Asset Freeze 12
5.2 Access to Frozen Funds 13
5.3 TFS Compliance Control 13

Part VI – On-site Inspections **13**

6.1 Annual Inspection Plan 13
6.2 Inspection Preparation 14
6.3 On-site Process 14
6.4 Closing Meeting 14

Parts VII – Tests, Controls, and Sampling **14**

7.1 How are Mechanisms Tested? 15
7.2 Sampling and Evidence 15

Part VIII – Corrective Measures, Sanctions, and Follow-up **15**

8.1 From Finding to Decision 16
8.2 Monitoring of Action Plans 16
8.3 Quality, Archiving, and Indicators 17

Conclusion of the Supervision Manual ***17***

Key Points Reaffirmed **17**

Preamble

This manual explains how SAMIFIN controls companies to prevent money laundering, terrorist financing, and the financing of weapons of mass destruction.

It describes what companies must do and how SAMIFIN verifies them, either remotely or directly on-site. The manual is primarily for SAMIFIN's teams, but it can also be used by other supervisory authorities and by the concerned companies themselves.

Important Terms

- **Risk-Based Approach (RBA):** Control efforts are focused where the risk is highest.
- **DNFBPs (EPNFD - *Entreprises et Professions Non Financières Désignées*):** These are businesses like real estate agencies, car dealers, jewelers, precious metal and stone dealers, etc.
- **VASPs (PSAV - *Prestataires de Services sur les Crypto-Actifs*):** Companies that offer services on virtual assets (crypto-assets).
- **STRs (DOS / STR - *Déclarations d'Opérations Suspectes*):** Suspicious Transaction Reports sent to SAMIFIN.
- **TFS (SFC - *Sanctions Financières Ciblées*):** Targeted Financial Sanctions, for example, freezing the accounts of an individual or company linked to terrorism.
- **Residual Risk:** Risk that remains after the company's control measures.
- **Grading:** Level of severity of a noted problem, from "minor" to "critical."

Who is Controlled and Where?

SAMIFIN primarily controls:

- Real estate agents
- Vehicle dealerships
- Dealers in precious metals and stones
- Jewelers
- Fund carriers/couriers
- Subjected professions for which no specific supervisory authority has been designated.
- Other professions that may be added by law.

These controls cover the entire country, with the possibility of including foreign subsidiaries if required by law.

Basic Principles of Supervision

SAMIFIN's working method is based on five simple ideas:

- **Focus on the strongest risks:** Riskiest types of clients, products, and countries.
- **Adapt the intensity of controls to the risk level:** More controls for high-risk companies.
- **Verify real effectiveness, not just paperwork and procedures.**
- **Protect information:** Professional secrecy and data security.

- **Work in coordination with other authorities and document everything properly.**

What the Manual Will Describe

The manual explains, step-by-step:

- How to evaluate a company's risk (likelihood, impact, risk before and after controls).
- What minimal data the company must provide (clients, products, countries, channels, etc.).
- How SAMIFIN selects companies for priority control.
- How remote (off-site) and on-site controls are conducted.
- How corrective measures and sanctions are decided.

Part I – Introduction

1.1 What is the purpose of this manual?

This manual explains how SAMIFIN controls certain companies to combat money laundering, terrorist financing, and the financing of weapons of mass destruction.

It translates laws and decrees into practical rules and simple steps for organizing controls, whether remote (off-site) or on-site. It is primarily intended for SAMIFIN's teams (analysts, inspectors, legal experts, IT specialists), but also for:

- Other supervisory authorities
- Monitored non-financial companies and professions
- Other involved government services.

This manual is regularly updated to account for changes in risks, laws, and practices.

1.2 Principles Guiding Supervision

SAMIFIN's supervision is based on 5 main principles.

- **Risk-Based Approach**
  - Efforts are concentrated where the risk is highest (clients, products, geographical areas).
  - Decisions are based on concrete data and regularly updated risk profiles.
- **Proportionality**
  - The higher the risk, the more frequent and in-depth the controls.
  - Low-risk entities receive lighter monitoring, except in case of suspicion.
- **Effectiveness**
  - Focus is on concrete results (e.g., timely Suspicious Transaction Reports, proper application of asset freezes), not just the existence of written procedures.
- **Confidentiality**
  - Information is protected and cannot be revealed to the persons concerned (prohibition of "tipping-off").
  - Access to data is limited to a "need-to-know" basis, and data is retained for at least five years.

- **Coordination**
  - SAMIFIN works with other national and international authorities to maintain a consistent approach.
  - All important decisions are written and justified (facts, analysis, legal basis).
- **Anchoring to the NRA (*National Risk Assessment*)**
  - The risk level of the NRA for each sector (low, medium, or high) serves as a starting point for organizing supervision.
  - SAMIFIN first sets a **minimum control frequency** based on this risk level, then adjusts this frequency according to the **specific risk** of each entity and warning signs (e.g., TFS, suspicion reports, recidivism).

1.3 Governance of the Manual

The manual relies on standard tools: risk matrices, report templates, questionnaires, and indicator grids. A decision-support matrix helps choose sanctions and follow-up actions in case of non-compliance.

The Director General of SAMIFIN approves the manual, which is reviewed at least once a year or as needed.

Any exception to the manual's rules must be explained and documented.

Exemptions and Special Cases Limited exemptions to certain supervision obligations or control frequencies may be considered only in well-justified cases, for example, for entities or activities presenting a very low risk, a very small size, or marginal activity volume. Any exemption must:

- Comply with current laws and decrees;
- Be based on a documented risk analysis (NRA, entity risk profile, nature of activities);
- Be approved by the competent hierarchical level (SAMIFIN Directorate);
- Clearly specify its scope, its potential duration, and the conditions for review.

Exemptions are never possible for entities or activities classified as high-risk, nor for essential obligations such as:

- Identification of clients and beneficial owners,
- Reporting of suspicious transactions,
- Application of targeted financial sanctions.

Part II – Laws and Institutions

2.1 Main Laws

The legal basis for supervision includes:

- **Law No. 2018-043 modified by Law No. 2023-026**

    - Sets the rules for combating money laundering and terrorist financing;
    - Imposes the risk-based approach on all subject entities;
    - Mandates Know Your Customer (KYC), identification of beneficial owners, and retention of documents for at least five years;
    - Imposes the reporting of suspicious transactions and prohibits tipping-off;
    - Provides for administrative and criminal sanctions (freezing, seizure, confiscation).
- **Decree No. 2024-1352**
    - Specifies that the National Risk Assessment (NRA) must be updated every five years;
    - Requires groups to conduct risk assessments at the group level;
    - Details the identification and updating of beneficial owners;
    - Specifies the roles of sectoral supervisory authorities.
- **Decree No. 2025-171 on Targeted Financial Sanctions (TFS)**
    - Creates the National Targeted Financial Sanctions Committee (CNSFC);
    - Requires asset freezing to be automatic, without warning the person, within 24 hours of designation by the UN or at the national level;
    - Provides that supervisory authorities must verify the application of TFS in their supervision.

2.2 Who Does What Nationally?

- **SAMIFIN:**
    - Receives, analyzes, and transmits suspicious transaction reports;
    - Is the supervisory authority for certain DNFBPs (real estate, car dealers, jewelers, precious metal and stone dealers, fund carriers, etc.);
    - Receives reports of asset freezes within the framework of targeted financial sanctions.
- **CNSFC:**
    - Proposes the listing or delisting of individuals or entities from terrorist lists;
    - Rules on requests for access to certain frozen funds within short deadlines.
- **ARAI (*Agence de Recouvrement des Avoirs Illicites* - Agency for the Recovery of Illicit Assets):**
    - Implements targeted financial sanctions;
    - Receives freezing orders, transmits them to the subject entities, and monitors their execution.
- **Sectoral Supervisory Authorities (e.g., CSBF, Ministry of Justice, etc.):**
    - Control the sectors falling under their competence, also applying the risk-based approach.
- **Prosecutor's Office and Investigative Forces:**
    - Conduct criminal prosecutions and investigations into offenses and transmitted cases.

2.3 International Cooperation

SAMIFIN and its partners use several channels:

- The Egmont Group for exchanging information with other Financial Intelligence Units (FIUs);

- Bilateral partnership agreements;
- The United Nations system and its sanctions committees;
- Channels for mutual legal assistance and international cooperation.

All this cooperation respects strict confidentiality rules.

Part III – Risk-Based Supervision Model

3.1 The Three Key Ideas of Risk

SAMIFIN's supervision model follows FATF standards and is based on three simple questions:

- **What are the threats?**
  - Criminal activities (drug trafficking, fraud, corruption, etc.);
  - Methods used by criminals (use of cash, shell companies, complex schemes).
- **What are the weaknesses (vulnerabilities) of the entities?**
  - Absence or weakness of customer due diligence procedures;
  - Poorly configured sanctions screening;
  - Insufficient IT tools;
  - Lack of staff training.
- **What would be the consequences if the risk materializes?**
  - Financial losses;
  - Reputational damage;
  - Legal sanctions;
  - Risks to the stability of the financial system and national security.

3.2 How is Risk Simply Calculated?

The model uses four steps:

- **Probability (P):**
  - Measures the chance that the risk will occur;
  - Rated from 1 to 4 (1 = low, 4 = very high).
- **Impact (I):**
  - Measures the severity if the risk occurs;
  - Rated from 1 to 4.
- **Inherent Risk (IR):**
  - Risk before taking into account the entity's controls;
  - Obtained by combining P and I, using the formula: IR=P×I (implied by the context).
- **Residual Risk (RR):**
  - Risk that remains after taking into account the quality of internal controls;
  - Used to classify entities as low, medium, or high risk.

The system uses a matrix that shows the risk levels and helps choose control priorities.

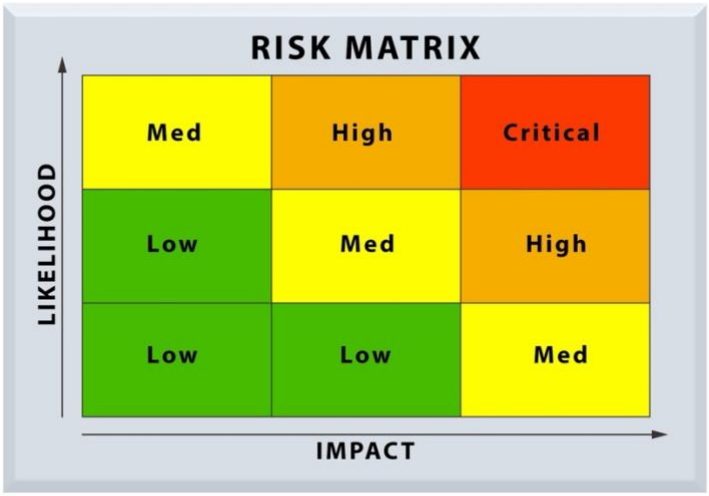


Figure 1 : Risk matrix

In practice, the risk level of each entity takes into account:

- Its **own profile** (clients, products, channels, countries, quality of internal controls), and
- The **risk level attributed to its sector** in the National Risk Assessment (NRA).

The sectoral risk level from the NRA (low, medium, or high) serves as the **starting point**, and is then adjusted according to the characteristics and the **residual risk (RR) score** of each DNFBP. This ensures consistency between the individual supervision of entities and the overall national risk view.

To ensure this consistency with the NRA, the residual risk score of each entity RRentity is adjusted by a **sectoral weighting factor** linked to the NRA risk level of the sector to which it belongs. The manual uses the following weighting coefficients:

- Sector classified as **High Risk** in the NRA: Factor **1.3**
- Sector classified as **Medium Risk**: Factor **1.0**
- Sector classified as **Low Risk**: Factor **0.7**

The entity's adjusted score is then calculated simply as follows:

Adjusted Score=RRentity×Sectoral Weighting Factor

This adjusted score is used to determine the **final risk category** (low, medium, high) and, consequently, the **frequency and intensity of supervision**, in accordance with the rules set by the manual (for example: annual visits, every 3 years, every 5 years, depending on the risk level).

3.3 Minimum Data to be Provided

To properly apply this approach, each entity must provide a minimum set of data, for example:

- **On its structure and governance** (shareholders, beneficial owner, organization chart, staff, internal control mechanisms);
- **On its clients** (number of high-risk clients, PEPs, clients who use a lot of cash, etc.);
- **On its products and services** (presence of cash, virtual assets, international transfers, remote operations);
- **On the countries and areas** it works with (high-risk countries, sensitive areas);
- **On distribution channels** (branches, internet, partners, trade shows, fairs, etc.).

SAMIFIN also looks at the **quality of controls**: CDD/EDD procedures, transaction monitoring, speed of suspicious transaction reports, implementation of targeted financial sanctions, compliance with deadlines (e.g., executing a freeze in less than 24 hours).

3.4 Application of the Risk-Based Approach

The legal framework stipulates that supervisory and control authorities (or, failing that, the Financial Intelligence Unit) must adopt a **risk-based approach** in their supervision missions of DNFBPs.

In application of this provision, SAMIFIN has developed this **Risk-Based Supervision (RBS) manual**, which specifies that the intensity and frequency of controls depend on the **specific risk profile of each entity**.

This approach implies that the **nature and depth of controls are modulated** according to the **residual risk (RR) score** of each entity. Establishing and regularly updating this profile makes it possible to adjust the **frequency and scope of inspections** based on:

- The evolution of risks,
- The type of activity,
- And the specific characteristics of each DNFBP (size, volume of operations, clientele, products offered, diversity, number, etc.).

Article 13 of Decree No. 2024-1352 reinforces this requirement by specifying that control authorities must **analyze risks and update the assessment** of reporting entities at a frequency set in their supervision manuals. This provision ensures the effective implementation of the risk-based approach by formalizing the periodic revision of assessments and thus the adjustment of control plans.

On this basis, the manual applies the following rules according to the residual risk (RR) level of each DNFBP:

Risk Level	Criterion (RR)	Frequency and Nature of Control

High	RR ≥ 3.00	* Annual on-site inspection; * Enhanced off-site supervision every 6 months (update of risk profile and overall assessment); * Quarterly meetings with General Management; * On-site controls focus on critical areas: transaction monitoring (TM/STR), targeted financial sanctions (TFS), customer due diligence (KYC/EDD), and governance.
Medium	2.00 ≤ RR < 3.00	* On-site inspection every 36 months; * Off-site supervision every year (assessment update); * Inspections may be thematic or targeted.
Low	RR < 2.00	* Documentary review (desk-review) every 2 years (risk assessment update); * On-site inspection every 5 years, primarily focused on sectoral awareness and basic compliance.

Part IV – Off-site Supervision

4.1 What is the purpose of off-site control?

Off-site control is the first step of supervision. Entities send information to SAMIFIN, which analyzes it without visiting the premises.

This analysis is used to identify risks, trigger alerts, and decide whether to:

- Conduct an on-site inspection,
- Request further explanations,
- Or impose an action plan.

Off-site control is also used to **update the residual risk (RR) level** and the **NRA-adjusted RR** of each entity. The information periodically received allows for adjustment of the risk profile and, consequently, the **frequency and intensity of future controls**, in accordance with the risk-based approach provided for in the manual.

Any significant change to the risk profile or the RR score must be tracked in the supervision file (reasons, data used, decision).

4.2 The Off-site Questionnaire

Entities complete a structured questionnaire divided into 6 blocks:

- **Institution:** General information, licenses, shareholders, beneficial owner, organization chart, staff.
- **Clientele:** Number of clients, high-risk clients, PEPs, NGOs, VASPs, etc.
- **Products and Services:** Which products are offered, which are the riskiest (cash, crypto, international transfers, etc.).
- **Distribution Channels:** Branches, internet, intermediaries, trade shows, etc.
- **Geographical Risks:** Relationships with high-risk countries or areas.
- **AML/CFT Mechanisms:** Sanctions screening, transaction monitoring, suspicious transaction reports, document retention, compliance officer.

Each question requires an answer, possibly a comment, and supporting documents, along with a brief definition for technical terms.

4.3 Document Verification

The attached documents (policies, procedures, minutes, audit reports, etc.) are checked to see if they are:

- Compliant with laws and decrees
- Consistent with the **National Risk Assessment (NRA)**
- Up-to-date and actually applied.

4.4 Indicators and Alert Levels

For each block, SAMIFIN reviews indicators (percentages, amounts, deadlines) and alert thresholds.

Depending on the severity, problems are classified as minor, moderate, major, or critical, with a color (yellow, orange, dark red) and possible follow-up actions (request for information, action plan, inspection, sanction).

Examples of alerts:

- Expired licenses or non-compliant legal status
- Too many cash payments compared to the sector
- Significant presence of PEP clients without enhanced controls
- Transactions with sanctioned countries not blocked
- Non-compliance with the 24-hour deadline for an asset freeze.

4.5 Analysis, Dialogue, and Follow-up

Off-site data is used to:

- Compare entities with each other
- Identify abnormal situations
- Decide on on-site inspections and priorities.

SAMIFIN organizes regular dialogue with entities (management, compliance, internal audit) and can:

- Request clarifications
- Impose an action plan with deadlines
- Launch a targeted or general inspection
- Apply corrective measures or sanctions.

A file is only truly closed when proof of correction is received and indicators become stable again.

Part V – Targeted Financial Sanctions (TFS) and CNSFC

5.1 From Designation to Asset Freeze

Targeted Financial Sanctions are based on:

- UN lists (terrorism, proliferation, etc.)
- The national list decided by the National TFS Committee (CNSFC)
- Possible requests from third-party States.

In summary:

1. An individual or entity is **designated** (UN or national).
2. The CNSFC decides, and ministers sign an inter-ministerial order.
3. SAMIFIN transmits the order to ARAI.
4. ARAI notifies the subject entities.
5. Entities must **execute the freeze immediately** upon receipt and in any case **no later than 24 hours** after the designation.
6. They send an execution report to SAMIFIN and ARAI.

All this must be time-stamped at each stage.

5.2 Access to Frozen Funds

Listed individuals or entities may request limited access to their funds for basic needs or exceptional expenses, or request to be delisted.

Requests are made to SAMIFIN (for the national list) or the UN sanctions committee, and orders for unfreezing or partial access are executed immediately by the subject entities.

5.3 TFS Compliance Control

SAMIFIN monitors in particular:

- The number and amounts of freezes
- Compliance with the **24-hour deadline**
- The number of blocked transaction attempts
- Delistings and processing times.

It also verifies, remotely and on-site, that the lists are properly updated, that freezes are executed within the deadlines, and that reports are transmitted.

Part VI – On-site Inspections

6.1 Annual Inspection Plan

Each year, SAMIFIN plans on-site inspections by combining:

- The risk level of the sector (NRA)
- The specific risk of each entity
- Warning signs: serious problems with TFS, STRs, recidivism, delays, etc.

The riskiest sectors and entities with the highest risk scores are visited first.

6.2 Inspection Preparation

Before visiting the site, SAMIFIN:

- Sends an announcement letter 21 to 30 days prior, stating the purpose, legal basis, dates, and documents to prepare
- Prepares an internal note summarizing the entity's risk profile and the points to be checked
- Requests data in advance (alerts, sanctions logs, proof of freeze, TFS reports...)
- Defines the samples of client files and transactions to be checked (high-risk clients, PEPs, cash transactions, sanctioned countries, etc.).

6.3 On-site Process

The inspection includes several stages:

- **Opening meeting** with management and key personnel.
- **Interviews** with management, compliance, audit, operations, and IT to verify the "culture of compliance."
- **Tests** on client files (KYC, beneficial owner, PEPs, document retention) and on risky products/services.
- **Control of channels** (intermediaries, digital) and suspicious transaction reports (quality, deadlines, absence of tipping-off).
- **Detailed tests on targeted financial sanctions** (list updates, blockings, freezes in less than 24 hours, reports sent).

"Walkthroughs" (complete journeys) are conducted to follow a case from start to finish, for example, from the first client contact to the suspicious transaction report.

6.4 Closing Meeting

At the end of the mission, the team presents:

- Findings classified by **severity** (critical, major, moderate, minor), with evidence and relevant legal articles
- Immediate measures to be taken if necessary
- The timetable for the entity to prepare an action plan (with steps and indicators).

Serious failures, particularly concerning TFS or STRs, may directly lead to sanctions and/or transmission to the public prosecutor's office.

Parts VII – Tests, Controls, and Sampling

7.1 How are Mechanisms Tested?

The manual describes, for each major theme (KYC/EDD, transaction monitoring, sanctions, document retention, specific sectors like NMPP - *precious metals and stones dealers*), how to control:

- **Objectives:** What the entity must concretely do
- **Legal references**
- **Indicators** to monitor remotely (off-site)
- **Tests** to perform on-site
- What is considered minor, moderate, major, or critical.

Examples:

- **KYC/EDD:** Verify that clients and beneficial owners are properly identified, and that PEPs have enhanced controls and management validation.
- **TM/STR:** Verify that the monitoring system effectively detects risky transactions and that suspicious transaction reports are sent quickly and filled out correctly.
- **TFS:** Verify list updates, freezes executed in under 24 hours, the existence of registers of attempts, and the sending of reports to SAMIFIN.
- **Document Retention:** Verify that requested files can be retrieved in a timely manner, for at least five years.

Critical failures (e.g., absence of a monitoring system, non-execution of a freeze, non-reporting of clearly suspicious transactions) systematically trigger strong follow-up actions.

7.2 Sampling and Evidence

SAMIFIN uses a "**sampling matrix**" to select the files and transactions to verify, focusing on:

- **High-Risk Clients (HRP)** and **PEPs**
- **High-risk countries**
- **Cash transactions** above certain amounts
- **Cross-border and digital operations**
- Cases where alerts have already been raised off-site.

The higher the entity's residual risk, the larger the sample.

In case of recidivism or non-compliance with previous action plans, the sample size is increased. Every sampling choice is documented (who, when, how) to maintain good traceability.

Part VIII – Corrective Measures, Sanctions, and Follow-up

8.1 From Finding to Decision

After an inspection or an off-site control, the findings are analyzed and classified according to their severity.

A "**decision matrix**" helps choose between: simple reminder, action plan, injunction, administrative sanction, or transmission to the public prosecutor's office.

Table 2: Sanctions Decision Matrix

Severity Level (Grading)	Type of Failure	Typical Corrective Measure
Minor	Formal defects, administrative errors.	Simple reminder or letter of recommendation.
Moderate	Weakness in the application of procedures.	Action plan with a deadline.
Major	Systemic failure or recidivism on an essential obligation (e.g., TFS not regularly tested).	Injunction, administrative sanction.
Critical	Fundamental failure (e.g., non-execution of an asset freeze within 24 hours).	Severe administrative sanction and immediate transmission to the Public Prosecutor's Office.

A sanction file always contains:

- The **legal texts violated**
- The **facts and amounts concerned**
- The **analysis of the risk created**
- The **measures imposed** (who does what, by when, with what evidence)
- The **deadlines and penalties** in case of non-compliance
- The **avenues of appeal**.

Failures related to targeted financial sanctions are treated with particular attention.

8.2 Monitoring of Action Plans

Post-inspection follow-up is continuous:

- Each action is tracked in a **dashboard** (green, orange, red)
- Controls are **more frequent** for major or critical findings
- A finding can only be **closed** with solid evidence (retests, time-stamped screenshots, audit reports, etc.).

In case of **repeated delays or failure** of the action plan, the file is automatically escalated to a **stronger sanction**.

8.3 Quality, Archiving, and Indicators

All decisions are recorded, and files are **retained for at least five years**, with limited access.

SAMIFIN also tracks its **own performance** (decision deadlines, entity compliance rate, recidivism, speed of TFS freezes) to improve its supervision mechanism each year.

Conclusion of the Supervision Manual

This manual formalizes SAMIFIN's approach in the fight against money laundering, terrorist financing, and proliferation. It establishes a clear, consistent, and **Risk-Based Approach (RBA)** supervision framework, ensuring that our resources are concentrated where the threats are highest.

Key Points Reaffirmed

- **Focus on Residual Risk:** The intensity and frequency of controls (off-site and on-site) are directly proportional to the adjusted risk score of each entity, ensuring fair and effective monitoring.
- **Commitment to Effectiveness:** SAMIFIN is committed to assessing entities' mechanisms based on their concrete results—notably the promptness in executing Targeted Financial Sanctions (TFS) and the quality of Suspicious Transaction Reports (STRs)—and not merely on the existence of written procedures.
- **Process Transparency:** From the initial assessment via the off-site questionnaire to the on-site inspection and sanctions follow-up, all steps are clearly defined and documented, ensuring traceability and consistency of decisions.

This manual is not static; it is an evolving document that will be updated annually or as needed to adapt to new threats, legislative changes, and international best practices. Its rigorous application by SAMIFIN's teams, in collaboration with other authorities and subject entities, is essential to strengthening the integrity of the financial system and national security.

SAMIFIN remains committed to ensuring robust, proportionate, and effective supervision, making every entity an active partner in defense against financial abuse.