

AMLYZE

 **Guide**

What data to prepare for your inspection?

Transaction monitoring

A brief guide for financial sector companies from the hands of regulatory insiders



Content

<u>Introduction</u>	03
AML/CFT software and tools used	04
Effectiveness and efficiency of transaction monitoring	07
Metrics to evaluate transaction monitoring effectiveness and efficiency	08
Data to be provided for inspectors for further client sampling	11

Introduction

Data is the new oil. It's valuable, but if unrefined, it cannot really be used.

Clive Humby, British mathematician



Regulatory inspections can be stressful for compliance staff, even if the organization's AML/CFT system is operating effectively and without significant concerns.

However, there is a simple way to alleviate this tension, and it revolves around adequately preparing data for the impending regulatory inspection.

A well-organized dataset not only helps compliance staff identify patterns, trends and potential risk areas within the institution, but also streamlines efforts during the on-site inspection. This makes the process more efficient and less resource-intensive, ultimately easing the burden on the compliance staff of the institution being inspected.

In our view, data is the fundamental basis for assessing an institution's AML/CFT health. Half of the work involved in an on-site inspection is the collection and validation of data to ensure that inspectors have the information they need. Here are some tips to help you prepare the necessary data points and meet the challenges of an on-site inspection with confidence. Remember that it takes time and effort to set up a system where everything is readily available.

In this guide, we will provide an overview of a specific aspect of the inspection data collection process, focusing primarily on transaction monitoring.

AML/CFT software and tools used

We will start our tutorial with some basic information that inspectors would gather about automated tools and software used for AML/CFT purposes. After all, this is where the data is collected, organized and processed for AML/CFT purposes. It's important to note that poor integration of these automated tools into an institution's governance framework can lead to data distortion and compromise the overall effectiveness of AML/CFT controls.

Furthermore, if users of the system do not understand its operating principles and make uninformed changes (e.g. adjusting parameters of the transaction monitoring system or sensitivity settings of sanctions screening algorithms) without considering the potential consequences, this could lead to regulatory sanctions due to the reduced performance of the system.

Of course, regulatory inspection will be interested in the tools and software used for AML/CFT purposes. Below is a summary of the information that supervisors typically review to assess the functionality of AML/CFT software. It's important to note that supervisors may delve deeper into any aspect and request further detailed information. Supervisors are likely to be interested in reviewing contracts with vendors if the institution relies on them for transaction monitoring.



AML/CFT software and tools used

Information on the automated tools used for AML/CFT purposes

Basic information

- ✓ **Purpose of the software/tool** [e.g. client identification; client risk scoring; transaction monitoring; fraud monitoring; sanctions/ PEP/ adverse media screening]
- ✓ **User roles:** [List of user roles with brief descriptions, e.g., administrator, analyst, reviewer, etc.]
- ✓ **User manuals,** guidelines and/or training materials

Data inputs

- ✓ **Sources of data that are uploaded to the system** [e.g. customer relationship management system, core banking system, payment processing system, etc.]
- ✓ **Frequency and methods of data updates**
- ✓ **Data reconciliation procedures**
- ✓ **Data retention procedures**

AML/CFT software and tools used

Information on the automated tools used for AML/CFT purposes

Incident management

- ✓ **SLA agreements**
[incident response and resolution times; agreement on service availability; performance metrics; scalability and performance; data backup and recovery etc.]
- ✓ **Business continuity management**
[in case of system malfunctions what are the solutions to ensure the continuity of the processes, especially for sanctions screening and real-time monitoring]
- ✓ **Information on major operational risk incidents that affected the transaction monitoring tools performance**
[the date of the incident; reasons of the incident; processes affected by the incident (including clients and operations affected); actions taken to resolve the incident; actions taken to prevent similar incidents]

Testing of the system

- ✓ **Testing documentation**
[testing plans, testing results etc.]
- ✓ **Functional testing**
[UAT, regular testing]
- ✓ **Performance testing**
[regular testing on how well the system functions]
- ✓ **Security testing**
[usually are out of scope of AML/CFT inspections, however might be included when there are specific security concerns]

Effectiveness and efficiency of transaction monitoring

Measuring the effectiveness and efficiency of AML/CFT transaction monitoring rules is critical to ensuring that financial institutions are able to detect and prevent illicit financial activities while managing costs and operational resources efficiently.

Different supervisors use different methodologies to indicate whether transactions are being monitored effectively. In our experience, common approaches include evaluating transaction monitoring procedures, analyzing specific transaction monitoring metrics, and conducting customer sampling to test the responsiveness of transaction monitoring rules to unusual or suspicious patterns of customer activity.

In certain cases, supervisors may use various IT tools to conduct comprehensive sampling and analyze the effectiveness of transaction monitoring rules in addressing specific typologies. We will take a simplified approach by focusing on the prerequisites for collecting specific information on **transaction monitoring metrics** and **sampling client transaction activity**.



Effectiveness and efficiency of transaction monitoring

Metrics to evaluate transaction monitoring effectiveness and efficiency

Here is the list of metrics that you may find useful to be prepared for the inspection.

1. Rule library

Rule name	
Rule activation period, dates of changes, reasons for deactivation or changes (if any)	[from-to] [deactivated from-to] [changes made: date] [reasons for deactivation or changes]
ML/TF typology to be covered by the rule	[transaction splitting; potential fraud; transit transactions etc.]
Rule objective	[e.g. freezing transaction; rejecting transaction; evaluating transaction retrospectively]
Coverage of the rule	Based on customer segment [individually monitored customers or group of customers; specific customer segments based on their industries, risk category etc.], operations [SEPA; SCT Inst; SWIFT; payment initiation services; lending operations; cash operations; card operations; etc.], geographies
Rule settings within the system	[rule code, rule parameters]

Effectiveness and efficiency of transaction monitoring

Metrics to evaluate transaction monitoring effectiveness and efficiency

Here is the list of metrics that you may find useful to be prepared for the inspection.

2. Transaction monitoring

(N.B. not including sanctions/PEP/adverse media lists)

Lists that are being used for transaction monitoring	[name based lists; IP based lists etc.] [whitelists; watchlists; blacklists etc.] [lists used for real-time or retro TM]
Authorized persons to make changes of the lists	
List coverage	[potential risks that are being covered by the lists in question]
List review and validation	[date of validation; method of validation; actions taken etc.]
Logs of the changes for the inspected period	[content of the change; date of the change; person who made changes]

Effectiveness and efficiency of transaction monitoring

Metrics to evaluate transaction monitoring effectiveness and efficiency

Here is the list of metrics that you may find useful to be prepared for the inspection.

3. Effectiveness

Used for the inspected period and the resolution time

Rule name	
Number of generated alerts	[a metric on closed alerts and open alerts might be included]
Number of alerts closed as false positive	[different metrics might be used, e.g.: - number of alerts discarded at alert analysis stage; - number of alerts discarded after investigation]
Average alert resolution time	
Number of the internal investigations carried out based on the alert	
Number of suspicious transaction reports based on the alert	

4. Testing

Information on testing of the rules for the inspected period

Type and scope of the test performed	[initial user acceptance tests; rule functionality tests (whenever new rule included); rule performance tests (e.g. based on historical data) etc.]
Date of tests performed	
Documentation of the results of the test (if any)	[the document or log in the system that indicates the results of the tests]
Actions taken after the tests	[e.g. rule deactivation; changes of the parameterization of the rule; changes of the coverage of the rule]

Effectiveness and efficiency of transaction monitoring

Data to be provided for inspectors for further client sampling

As noted above, a common method of assessing the effectiveness of transaction monitoring rules is to review a sample of client files. Inspectors may review transaction activity within selected client relationships, examining specific transactions and related monitoring documentation to determine whether the institution has identified and reported suspicious activity.

Suspicious patterns may be identified through automated transaction monitoring rules that trigger alerts, as well as through subsequent investigation. In this article, however, we take a simplified approach and do not delve into the intricacies of alert investigation. Instead, we provide the key data points necessary for supervisors to draw a sample for review.

Please note that institutions are required to provide high quality data for a large number of clients. Supervisors typically validate the data before drawing a sample, and any concerns about data quality during an inspection may raise doubts about the overall quality of the data provided and possible data manipulation. This could lead to the conclusion that the institution is uncooperative and avoids providing necessary data for inspection purposes. Ensuring data quality is therefore critical to maintaining compliance and demonstrating cooperation during supervisory inspections.



Effectiveness and efficiency of transaction monitoring

Data to be provided for inspectors for further client sampling

The following may be requested in order to take a sample of the client file for further testing

✓ Client ID and name

✓ Client type

[natural person/ legal person]

✓ Client transactional turnover For inspected period

[the following segregation might be requested:

- number of incoming transactions;
- number of outgoing transactions;
- value of incoming transactions;
- value of outgoing transactions;
- the respective currency in which operations have been carried out]

✓ The financial products the client is using

[local payments; cross-border payments; lending; trade based financing products etc.]

✓ Country of residency

[based on the local understanding, what “residency” means;
for legal persons country of residency of UBO might also be requested]

✓ Duration of business relationship

[start date; end date (if any)]

✓ Industry of activities For legal persons

✓ Risk group of the client

[dates of changes might be requested; risk group defined during onboarding might be requested]

✓ Type of client due diligence carried out

[e.g. if CDD/ODD/ EDD during the inspected period has been carried out]

✓ If any internal investigations has been carried out and STRs provided

[the number might be requested as well]

Sampling criteria that are common during the on-site inspection

The criteria for sampling may vary, as may the methods for sampling (as mentioned above, advanced sampling tools may be used). For the sake of simplicity, we provide you with some very obvious criteria that every supervisor takes into account:

- ✓ specific transaction/payment turnover of customers (e.g. customers with the highest turnover; customers divided into different turnover groups, etc.)
- ✓ the place of residence of the customers (e.g. domiciled in the institution's home country, in the European Union, in high-risk third countries identified by the European Commission, in countries included in the Financial Action Task Force (FATF) black or grey lists, etc.); and
- ✓ the place of residence of the ultimate beneficial owners (e.g. domiciled in the country of origin of the institution, in the European Union, in high-risk third countries identified by the European Commission, in countries included in the black or grey lists of the Financial Action Task Force (FATF), in destination countries, etc.);
- ✓ the individual risk rating of the customer (high, medium and low risk customers);
- ✓ the type of due diligence carried out on the customer (e.g. customers who have undergone enhanced due diligence);
- ✓ the complexity of the ownership structure of corporate customers (e.g. customers with complex ownership structures);
- ✓ the type of client (individual and corporate);
- ✓ the product used by the client;
- ✓ the length of the relationship with the client (for example, new clients);
- ✓ the industry in which the corporate customer operates (e.g. customers operating in high-risk industries);
- ✓ the channel used to serve the customer (e.g. customers who received financial services through intermediaries), etc.

Several combined criteria (e.g. size of turnover and customer residency) may be used for sampling purposes, but it is left to expert judgment and supervisory procedures to define the specific set of customers to be tested.

AMLYZE

Want to discuss it more?

**Book a meeting
with us at
amlyze.com**

LET'S TALK

