Deloitte.

# Approach for a Robust End-to-End Post-Event Transaction Monitoring Program

By: Christiaan Visser and Richard Bakkers

# Approach for a Robust End-to- End Post-Event Transaction Monitoring Program

The increasing costs of compliance as well as the improving technological capabilities drive the urge for a data-driven, scalable post-event Transaction Monitoring program. However, specifically in the Netherlands, recent regulatory investigations have exposed various shortcomings in post-event Transaction Monitoring programs within (international) financial institutions, including banks. Issues on both quality and efficiency can be solved by employing a structured and iterative process in managing a post-event Transaction Monitoring program.

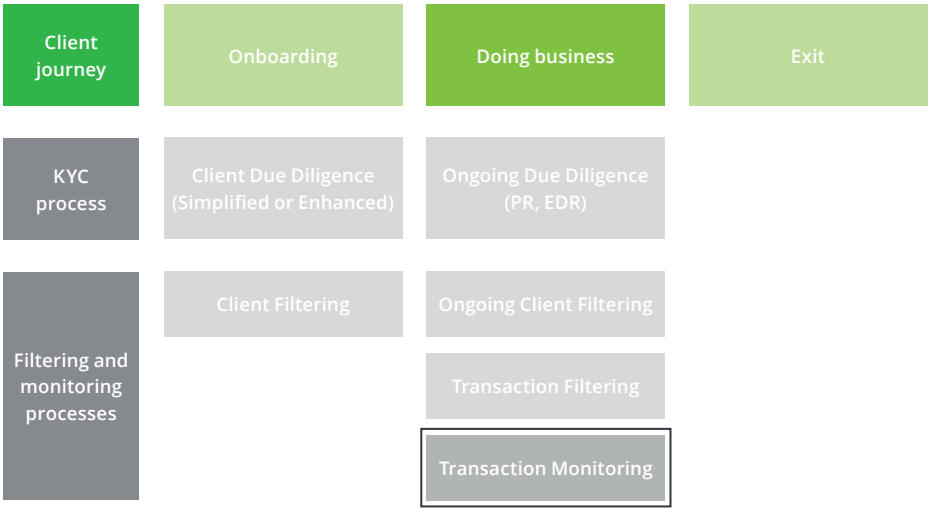
On 19 May 2017 the Dutch Central Bank published the concept of its guidance document on post-event Transaction Monitoring within banks. In short, the Dutch Central Bank has mentioned six components that can illustrate the maturity of post-event Transaction Monitoring implementation:

1. Risk Assessment & Risk Profile;
2. Policies & Procedures;
3. System & Business Rules;
4. Alert Handling & Suspicious Activity Reporting;
5. Governance;
6. Training & Awareness.

Deloitte has developed an approach that supports strengthening maturity levels of components 1, 3, and 4, making impact on the quality and efficiency of post-event Transaction Monitoring.

## Post-event transaction monitoring in context

As part of a broader Financial Economic Crime ('FEC') framework, post-event Transaction Monitoring is considered a powerful control to detect, further investigate & report (potential) suspicious transactions:




Post-event Transaction Monitoring is a control to meet AML/CTF requirements during the client lifecycle by detecting potential suspicious behavior

## Common pitfalls

Supporting various financial institutions with reviewing and strengthening their post-event Transaction Monitoring program, Deloitte has identified a number of common shortcomings:

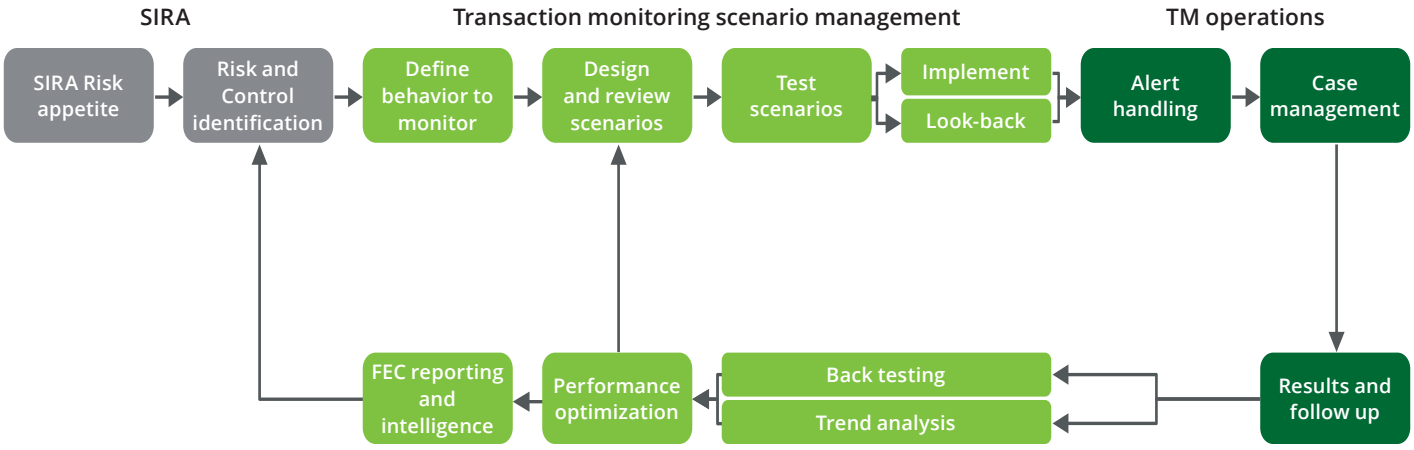
- Insufficient or inexplicit alignment with the Systematic Integrity Risk Analysis ('SIRA');
- Insufficient involvement of the 2nd line of defense during alert handling and case management;
- Not using client AML or CDD risk profiles in alert generation;
- Insufficient granularity and precision in defining the norm for expected behavior.

In our experience the root causes for these shortcomings are usually:

- Lack of robust governance ensuring end-to-end ownership;
- Lack of oversight;
- Lack of feedback loops to ensure continuous improvement;
- And, maybe the most important, the lack of a strategic view on the control Transaction Monitoring within FEC and their overall strategic goals.

## Deloitte's approach

Within Deloitte we have developed the following approach for a robust end-to-end post-event Transaction Monitoring program:




Using **SIRA**, Financial institutions:

- Monitor risk areas based on the characteristics of the business
- Identify risks inherent to their business
- Determine the mitigating effect of controls such as transaction monitoring
- Calculate residual risk
- Compare residual risk to risk appetite

**TM tooling** is configured and updated to detect potentially suspicious behaviour:

- This configuration based on risks identified in the SIRA
- Behavioural typologies that indicate identified risks help in accurately describing detection scenarios
- A feedback loop is used to ensure that the quality of alerts generated continuously improves
- Both what data to use, as well as setting when to produce an alert (thresholds), serve as 'dials' to further tune detection scenarios

**TM alerts** are to be processed to identify suspicious behaviour which can be use for:

- External reporting
- Continuous improvement

## SIRA alignment is key

Effective post-event Transaction Monitoring scenario management is based on the relevant FEC risks identified and assessed during the Systemic Integrity Risk Assessment (SIRA) , as well as up-to-date and complete FEC (client & transactional) data. Therefore a sound SIRA process and de availability of relevant data are key success factors. Furthermore, the process should not be seen as simply linear. Rather, the output of operational alert handling processes should be used as input for continuous improvement of the post-event Transaction Monitoring program. This approach allows financial institutions to specifically define which behavior and associated risks their post-event Transaction Monitoring scenarios need to monitor. More importantly, the approach allows financial institutions to do so not only effectively, but efficiently.

## Defining behavior to monitor

Modus operandi for risks identified in the SIRA for which post-event Transaction Monitoring is deemed a relevant control are identified, including related red flags which can be used to detect the associated behavior. Modus operandi should specify:

- Who - Client Type;
- What - High level description of the SIRA risk;
- How - What is the underlying client behavior (input for red flags).

The red flags are data points used to design the post-event Transaction Monitoring scenarios and are based on market practices, recent cases, point of views from (inter)national regulators and literature. Client, product, and transaction data, and especially availability thereof, form the cornerstone of this process.

## Design, Test & Implement Post- Event Transaction Monitoring Scenarios

The design phase includes the full functional and technical development process that delivers the monitoring scenarios in the post-event Transaction Monitoring solution. During the test phase the post-event Transaction Monitoring scenario design is tested.

Depending on the preferred project management framework (waterfall, agile, etc.) various testing activities can be performed in parallel to design activities. Lastly, a 'lookback' should be considered in parallel to the implementation of new or adjusted scenarios. The goal of the lookback process – that should be robust in itself in order to draw correct conclusions – is to determine if the financial institution has missed (potential) suspicious transactions in the past (i.e. before implementing the new/adjusted scenario). Usually, the initial lookback period is six months.

### Alert handling & continuous feedback loop to improve scenario effectiveness

After implementation of post-event Transaction Monitoring scenarios in production, output will be generated in the form of alerts. These alerts are typically assessed by first and second line of defense personnel to determine the potential presence of suspicious activity. Alerts deemed indicative of suspicious activity are commonly referred to as 'true positives'. Alerts for which the underlying behavior can be reasonably be explained to be appropriate are then referred to as 'false positives'. Operational costs can be reduced by optimizing scenarios so that that false positives are limited while preserving true positives.

Our approach incorporates a continuous feedback loop to facilitate this operational optimization. This feedback loop leverages alert handling information to fine-tune the scenario management process. These activities are commonly referred to as 'backtesting'. In the backtesting phase the effectiveness and quality of the alert definitions are periodically assessed. Backtesting consists of analytical observations (factual) and corresponding risk analyses, which entails more than only a basic true vs. false positive ratio.

Examples of backtesting methods are:

- Analysis of random samples of transactions or clients that did not produce alerts to detect possible 'false negatives';
- Comparison of other risk signals than Transaction Monitoring with Transaction Monitoring output;
- Using true and false positive data to identify additional data points to be used to identify true positives;
- Analysis of timeliness of alert handling and filing suspicious transaction reports.

**Further information**

The above is the description of a general approach that, of course, needs to be further tuned to (a.o.) your financial institution's clients, products and risk appetite.

Furthermore, Deloitte can support you with Transaction Monitoring related policies & procedures, governance and training & awareness (components 2, 5. and 6 as mentioned in the Dutch Central Bank's guidance document).

For further information you can contact:

**Christiaan Visser**
Director
chvisser@deloitte.nl
+31 (0)88 288 54 28

**Richard Bakkers**
Senior Manager
rbakkers@deloitte.nl
+31 (0)88 288 6972

Deloitte.