Towards Better Transaction Monitoring

March 2019

Contents

Towards Better Transaction Monitoring?

Criminals are becoming more and more sophisticated in their methods to disguise and conceal the origins of the proceeds of crime. At the same time, regulators are becoming more and more demanding of institutions they supervise over how they identify, prevent, monitor and disclose their suspicions when they are exploited for laundering criminal funds.

The news cycle relentlessly reports on more and more financial institutions being drawn into the workings of vast, global laundromat schemes that are facilitating the laundering of billions of dollars of illicit cash. As more details come to light, the nature and extent of the activity seems to have been hiding in plain sight.

Case Study 1: the power of transaction monitoring

In 2016, a Romanian money laundering and drug trafficking syndicate was operating in Australia. This group was suspected of using international fund transfers to Romania to fund the importing of narcotics into Australia and also to transfer the proceeds of crime out of Australia.

One key member of the syndicate would visit several remittance agents and banks to transfer money out to Romania. The transfers were all structured such that each transfer was below the AUD 10,000 reporting amount in an attempt to avoid detection.

However, reporting by financial institutions of suspicious transactions identified through their transaction monitoring programmes, combined with further investigation performed by AUSTRAC and Australian law enforcement agencies, enabled the disruption of this syndicate. The following indicators were identified:

- Multiple transfers were sent to common beneficiary customers in Romania.
- Multiple transfers were sent structured in amounts of less than AUD 10,000 in order to avoid cash threshold reporting obligations.
- Multiple transfers were sent by a single ordering customer on the same day, at different agent locations of the same remitter.
- The ordering customer of the transfers was also the receiving beneficiary overseas.
- False identification details were also used when conducting international transfers, identified by a variation in the addresses, phone numbers and dates of birth used when conducting transactions at separate remittance agent locations.

Ultimately the key syndicate member was arrested and charged with money laundering offences and other charges and was sentenced to 7 years and 4 months' imprisonment.

Source: http://www.austrac.gov.au/case-studies/austrac-helps-bust-money-laundering-syndicate

A strong transaction monitoring programme is a critical component in an effective anti-financial crime function. Identifying and investigating transactions and behaviours for indicators of illegal activity is an onerous and expensive exercise, but it shouldn't be a fruitless one. Financial Institutions are the first line of defence in an integrated system that also involves Governments, Regulators, Law Enforcement, Intelligence Agencies, Non-Governmental Organisations and supra-national bodies seeking to prevent, detect and prosecute illegal activities worldwide.

But such programmes are not cheap.
Over the years, the financial services industry has focused much of its investment in financial crime controls on the selection, implementation and optimisation of advanced, anti-money laundering (AML) transaction monitoring systems, often with varying success. Significant effort is also expended recovering from backlogs of alerts generated by those systems, many of which are false positives, when the implementation of those systems go wrong or get out of hand.

There are many reasons why programmes like this can go wrong. Third party systems may not live up to expectations placed on them, or poor data quality may mean that scenarios or rules cannot identify the activity they were intended to. More broadly, inadequate enterprise or customer risk assessment processes may mean that the proposed approach cannot ever deliver what was expected of them.

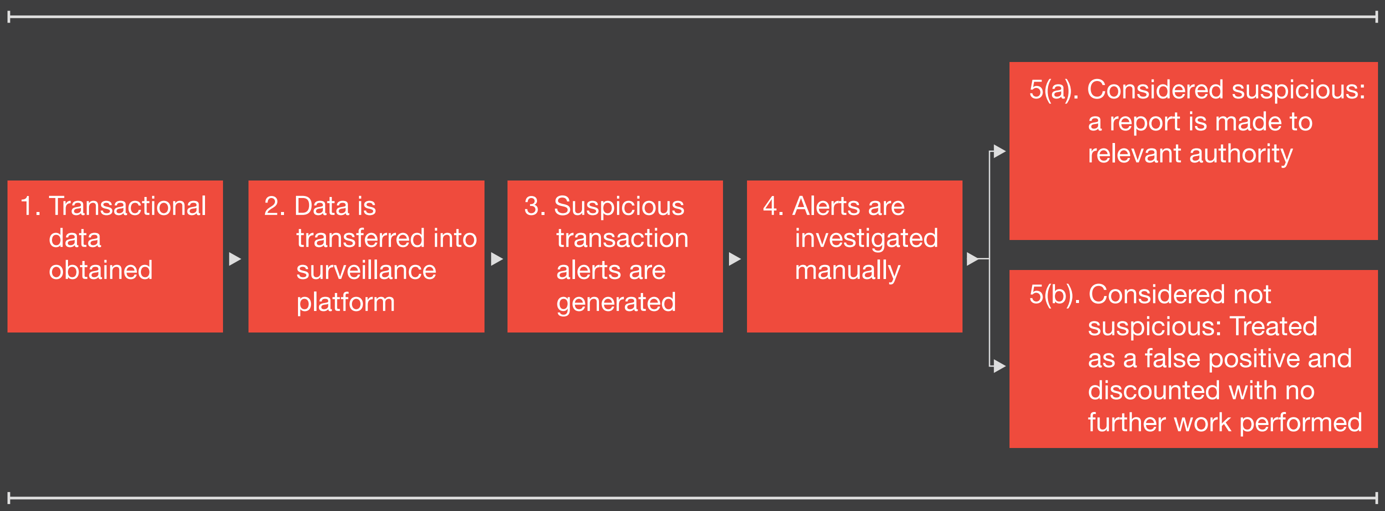
However, there is another missing piece of the puzzle. Our experience suggests that too many institutions have given too little attention thinking about how to most effectively investigate the alerts that are generated.
Too often, it is viewed as a manual, mundane task done to clear the noise generated upstream, rather than the important task of identifying genuine criminal behaviour.

Challenges in the transaction monitoring process

The approach to undertaking transaction monitoring in any financial institution is similar. Transactional data is ingested alongside other, relevant data sets into a monitoring platform. This data is then analysed against a set of rules or detection models, often referred to as 'scenarios'. The simplicity or complexity of these models varies according to the complexity and risk appetite of the financial institution, the nature of the underlying risks being monitored for, the profile of the underlying customers or products and the type of technology (or more often technologies) employed.

The output is a list of alerts associated to unusual transactions, behaviours or patterns exhibiting certain red flags, indicative of money laundering, terrorist financing or any other risks that are being monitored for. These are subjected to a manual review by analysts to determine whether or not these transactions, behaviours or patterns are truly suspicious, in which case a report will need to be made to the relevant authority. If the alert is not deemed to be suspicious it is discounted by the analyst and no further investigation is performed. Generally speaking the procedures performed above are all subject to some form of quality assurance within the organisation.

Figure 1. Standard high-level transaction monitoring process



1. Transactional data obtained

2. Data is transferred into surveillance platform

3. Suspicious transaction alerts are generated

4. Alerts are investigated manually

5(a). Considered suspicious: a report is made to relevant authority

5(b). Considered not suspicious: Treated as a false positive and discounted with no further work performed

However, as you get into the detail, there are challenges at every step of the way.

Financial institutions frequently struggle with the completeness and accuracy of data that they are using for the purposes of monitoring. Technology architecture has frequently grown by acquisition rather than organically, with new systems bolted on to old, creating a disparate and diverse landscape. Connecting the dots to ensure that all relevant information is obtained and presented in a useable format is difficult. Poor data integrity will also cause poor quality alerts, leaving financial institutions with a large number of unproductive alerts that are difficult to manage downstream.

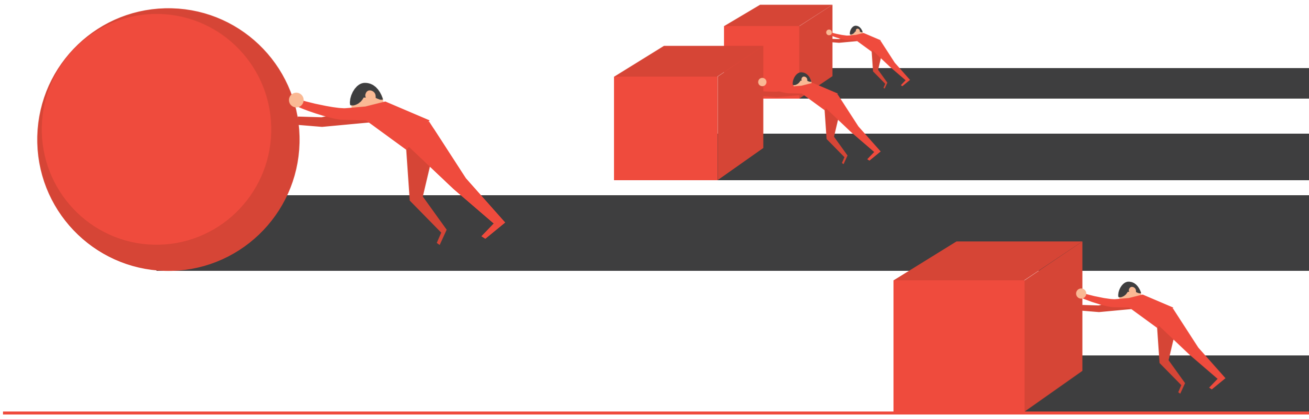
Institutions that have grown by acquisition may operate multiple platforms and therefore multiple processes to manage their obligations.

Alerts are generated through rules that often are uniformly applied for all of an institution's transactions and can be overly simplistic in their application. In the target state, scenarios should trigger alerts based not only on customer segments, but also on more detailed customer types, product types, transaction channels or the origin and destination of the flow of funds. There are numerous developments in this area with network analysis and behavioural analytics complementing more traditional rules based scenarios which can drive positive changes in this area.[1] Enhancements in all of these areas are key to achieving a best-in-class transaction monitoring programme. But what happens next?

Indicators of unusual activity, however generated, will eventually need to be reviewed by a human. Notwithstanding advances in technology, the reality is that for the foreseeable future there will remain a large component of human review. The United Nations Office on Drugs and Crime estimates that 2-5% of global GDP ($800bn - $2 trillion USD) is laundered through the financial system globally in a year.[2] Even if only a fraction of this can be identified by financial institutions as part of the transaction monitoring, that is a lot of activity to investigate.

Alert handling is an area where the industry to date has spent proportionately less time looking at improving quality and efficiency, in comparison to work performed elsewhere in the monitoring process. Alert handling is often seen as a straightforward, vanilla process when considered against exciting new technologies that promise dramatic decreases in the volumes of alerts being generated and therefore are typically more able to attract investment.

As a result of the relative lack of attention paid to the investigation process, there remains significant potential for improvement.



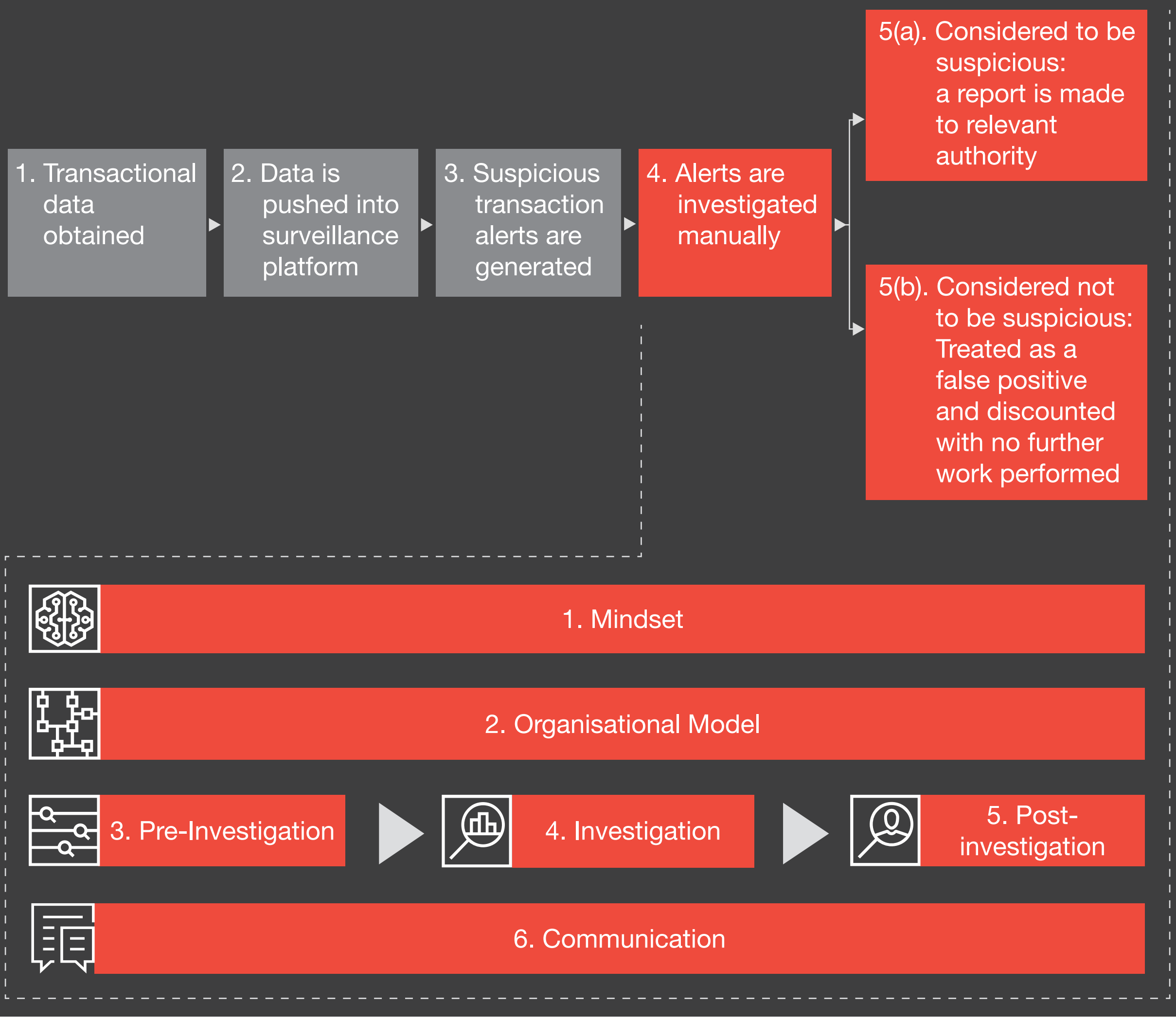
Successful alert handling

In our experience, successful alert handling requires action across 6 themes. Enhancing each of these areas will create robust processes that can mitigate risk. The core process can be broken down into pre-investigation activities, the investigation itself and then post-investigation activities. However, broader considerations centre on culture, identifying the organisational model itself and communication strategies. We will examine each of these areas in turn, the common pitfalls and areas where financial institutions can start to enhance their operating model activities.

[1] https://pwc.blogs.com/data/2018/05/transaction-monitoring-why-segments-and-thresholds-are-never-enough.html

[2] https://www.unodc.org/unodc/en/money-laundering/globalization.html

Figure 2. Six focus areas for improving transaction monitoring alert handling


1. Transactional data obtained
2. Data is pushed into surveillance platform
3. Suspicious transaction alerts are generated
4. Alerts are investigated manually
5(a). Considered to be suspicious: a report is made to relevant authority
5(b). Considered not to be suspicious: Treated as a false positive and discounted with no further work performed
1. Mindset
2. Organisational Model
3. Pre-Investigation
4. Investigation
5. Post-investigation
6. Communication

Mindset: why do we perform transaction monitoring?

It should be easy to motivate employees to fight financial crime if they recognise the impact that their work has on society by preventing and detecting criminal activity. However, financial institutions have often focussed on operational efficiency rather than the mitigation of the real risk. The process of investigating transaction monitoring alerts has become a time-bound, operational task rather than an attempt to stamp out financial crime. Simplistic, volume focussed Key Performance Indicators (KPIs) are used to measure staff performance and senior management, fearful of the large scale fines and regulatory censure that can result, put more focus on staff to complete large volumes of alert review in order to avoid falling behind.

This leaves staff more focused on the drudgery of clicking through waves of alerts every day rather than the true purpose of what they are doing – fighting financial crime. There should be focus at the senior management level not only on quantity and volume KPIs, but also on the quality of the investigation. Equally, staff performing these investigation activities need to be educated on the risks they are seeking to identify and mitigate and incentivised by the quality and efficiency of their investigation.

> “Each new alert must be viewed by staff as a potential indicator of the activities of a drug cartel or international people trafficking organisation or some other serious crime.

Key response:

- Enhanced KPIs
- Training for staff

This culture change must be enabled by shifting the conceptualisation of transaction monitoring from an operational task to a risk identification and mitigation exercise. Importantly, those tasked must be empowered through a clear understanding of the end-to-end transaction monitoring process and its objectives.[3]

This means understanding the typologies published by all stakeholders, the scenarios defined to detect them, the red flags to identify them and the investigation techniques to validate them. Traceability between all of these factors provides a platform for staff to perform a robust investigation, reach the correct decision and document a clear and comprehensive rationale. Each new alert must be viewed by staff as a potential indicator of the activities of a drug cartel or international people trafficking organisation or some other serious crime.

Organisational model: the right people for the right job

As the methods of committing financial crime evolve and change, regulators try to keep up by publishing the typologies that criminals employ as they are identified. These new typologies are used by financial institutions to update what they search for and are a necessary step to ensure that financial institutions and law enforcement keep up with the criminals trying to abuse the financial system. However, simply increasing the list of scenarios to monitor usually results in an increased number of alerts to investigate.

Key response:

- Detailed capacity model review with realistic assumptions
- Outsourcing

This is a common and well-known issue within the industry. How should financial institutions deal with large volumes of alerts? There is no silver bullet. New technologies provide part of the answer by providing new ways to analyse large amounts of data, providing more targeted results. However, such technologies take time to develop, test and embed in an organisation. In the meantime, there are a lot of alerts that require review. It is also the case for most organisations, that given their volume of transactions, a large number of alerts will always be generated.

The clear response that we have seen in the market is to get more people to clear the alerts. However, teams need to be structured appropriately. Having experienced staff performing manual, large volume tasks can be expensive, while having inexperienced staff in highly-skilled roles is clearly a recipe for disaster. A well-defined organisation structure, with clear roles and responsibilities is critical.

[3] This was flagged by the Monetary Authority of Singapore in recent guidance on transaction monitoring good practice. For further information, please visit: https://www.pwc.com/sg/en/financial-services/financial-crime/blogs/improve-risk-mgt-through-transaction-monitoring.html

Successful operating models effectively triage their staff to ensure that the more junior staff focus on the simpler, less risky alerts, while the most experienced staff focus on the high risk alerts and drafting of Suspicious Transaction Reports to regulators. Adopting a structured deployment of resources into smaller defined groups is particularly effective, where a group of analysts, quality reviewers and subject matter experts work together on a book of work in a cohesive manner, providing real-time checks and feedback.

A further advantage of adopting a structured deployment model is that it is easily scalable. The volumes of alerts can radically increase, either due to new typologies, as discussed above, or operational snags that cause backlogs. Teams can be mobilised quickly as discrete groups in order to ensure that alerts are handled in a timely manner.

Outsourcing this process to specialist providers can also provide an answer. Such teams can be mobilised at short notice to assist with immediate challenges or provide interim support while in-house teams develop and test new technologies. We believe that it is critical for financial institutions to keep expertise in house when it comes to analysing the identified suspicious activities and identifying any required changes in the transaction monitoring approach. As such, it is important that financial institutions ensure that their in-house teams are able to focus on the complex and higher risk alerts in order to determine what the organisation's preferred response should be.

The bottom line is that staffing and organisational structure must be sufficient and suitable in order to respond to the risks that the bank faces. When this is not the case, the repercussions can be severe for the organisation, as can be seen in the Case Study 2 ('When it goes wrong… Poor staffing')

Case study 2: when it goes wrong… insufficient and inexperienced staffing

- Multiple failings were identified by US regulators at one organisation in February 2018 relating, amongst other things, to poor staffing and organisational model decisions.
- Some of the failings identified were as follows:
  - Senior roles of Chief Compliance Officer and AML Officer, and other roles, were staffed by individuals with no or limited AML experience.
  - Only 25-32 AML investigators were part of the team to review and clear alerts, at a time when the bank had $340 billion in assets.
  - Despite complaints from Human Resources and Compliance personnel that AML investigators were being paid below market rates, salaries of certain AML staff failed to increase.
  - Despite requests from compliance personnel, the compliance team was forced to rely on obsolete systems, with funding for upgrades and replacements for computers and other hardware being denied.
  - The volume of alerts resulting from the transaction monitoring system was set such that the number of alerts was effectively capped at a specific volume, allegedly associated with the level that staffing capacity could cope with at the time. The OCC refers to 'resource-based alert caps'.

Source: https://www.sec.gov/Archives/edgar/data/36104/000119312518047256/d516835dex101.htm

Pre-Investigation: the tortoise and the hare

In our experience, teams at financial institutions are so keen to get started on the investigation in order to ensure they get through their required volume of alerts, that they often miss the pre-investigation step, with negative impacts felt further down the line. We see alerts coming out of the transaction monitoring system and immediately going into an analyst's work queue to be dealt with on a first-in-first-out basis.

The best transaction monitoring programmes are smarter than this, the slower methodical tortoise that beats the quick hare by the end of the long race.

Data should be enhanced with information from various relevant banking systems, thoroughly cleansed (from unnecessary or duplicated information) and presented in a clear well-organised form prior to being provided to the analyst for investigation. This way the analyst will see the holistic picture from the start of the investigation and will be able to focus on analysing, understanding and assessing the information. Instead, often the analyst's work focuses on jumping through the multitude of various systems and sources in search for the required data points, and the overall picture is not seen.

Key response:

- Review of logic used to batch alerts together for review
- Rules based auto-closures

Furthermore, having alerts organized in batches and enhanced by information from various sources, allows analysts to consider them holistically from the perspective of what the detection scenario was that triggered the alert in the first place, and whether the actual issuance of the alert is still valid.

Needless to say, any such decision needs to be well documented, and traceable. By applying advanced technologies (rules engine, machine learning and AI based solutions), such an analysis can be automated and be part of the pre-investigation activity.

Such pre-investigation analysis also allows organisations to prioritise alerts for review based on their own risk appetite. A common tenet of regulators around the world is that an organisation's response to financial crime must be risk based. Indeed, it is almost impossible to detect all wrongdoing. Agreeing a set of criteria to prioritise alerts allows organisations to deploy their resources according to the risk they perceive and to demonstrate to regulators that they are doing so.

Investigation: getting the right tools for the job

Each alert that is generated needs to be assessed and a conclusion reached as to whether it is a potential case of financial crime or not. This is an investigation, and like any investigation it must be conducted in a methodical and detailed manner.

Over the years, we have seen wide variation in the quality of what is performed and recorded as part of this investigation. In most instances, free text fields are left for analysts to document the steps undertaken and conclusions reached. Sometimes, these fields are completed in detail, however, more often these fields are filled with little to no rationale of how and why the conclusion was reached. In the majority of cases, this is not because no investigation was performed but instead simply poor documentation of the work that was performed. There are cases, however, when poor quality investigation has been identified by regulatory authorities, with severe implications for the organisations involved. Please refer to case study 3 below ('When it goes wrong: poor quality').

Key response:

- Negative news Artificial Intelligence
- Automation bots
- Workflow tool

Case study 3: when it goes wrong… poor quality

Investigations by the MAS and FINMA, the Swiss Financial Market Supervisory Authority found serious transaction monitoring failings at one organisation in relation to its role in the 1MDB corruption scandal.

- The investigation led to the withdrawal of the organisation's merchant bank status in Singapore, the first time this had been done since 1984. Financial penalties were also imposed and individuals were referred to public prosecutors.
- Similar censure was provided by FINMA, including the disgorgement of profits to the tune of CHF95m million.
- Amongst other failings, it was determined that there were significant shortcomings in the bank's transaction monitoring, with numerous large transactions being executed with no clear purpose and multiple red flags were ignored. Specific examples flagged by FINMA were:
    - The bank was happy to accept the client's explanation that the source of funds for a deposit of USD 20 million was a "gift"
    - An account was credited with CHF 98 million without any attempt to ascertain the commercial rationale for this credit
    - Transactions were executed that directly contradicted the stated purpose of the account as ascertained at the account opening stage
    - Transactions were explained as being related to loan agreements, when the agreements actually had no bearing on the real background to the transaction
    - USD 20million was routed through multiple accounts in the bank in one day before being sent out to another bank. The rationale provided was simply that these transfers were for "accounting purposes".

Source: https://www.finma.ch/en/news/2016/05/20160524-mm-bsi/
http://www.mas.gov.sg/News-and-Publications/Enforcement-Actions/2016/MAS-directs-BSI-Bank-to-shut-down-in-Singapore.aspx

Increasingly, we are seeing cross border cooperation between regulatory bodies. Under certain conditions, Financial Intelligence Units from around the globe can share information to assist in the detection of financial crime.[4] This can trigger a local regulator or law enforcement agency to request information from specific organisations in their territory. What if the activity in question was never identified as requiring investigation by the organisation? Or worse still, what if that activity was identified, investigated and disposed of as not suspicious?

So how do you ensure that the investigation performed by analysts is done with the appropriate care and rigour consistently and the results are traceable back to the steps performed? There are 3 key steps that we believe help to achieve this:

1. Gather data

In order to perform a detailed investigation, analysts need to collect, connect and process information from a number of internal and external sources. The way in which many financial institutions' systems have been established makes the data collection for customers, transactions, alerts and related parties information extremely manual. This is compounded by the number of external sources that the investigator has to search and the manual effort required to analyse and disposition results. There are automated technology solutions available in the market that can automatically collate a consolidated view of the relevant internal and external information.

2. Provide guidance and training

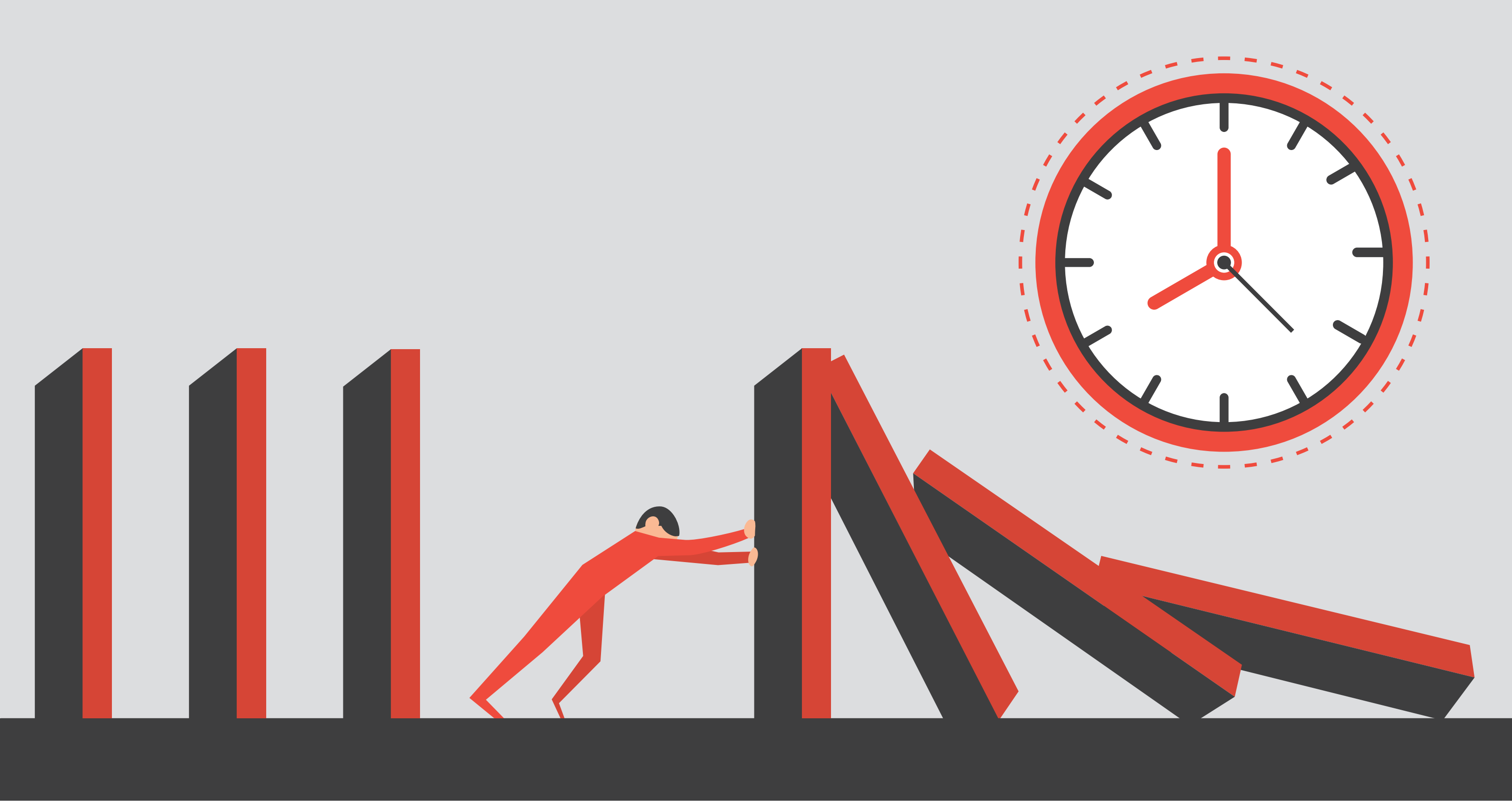
Many investigations lack structure. Often there are different documentation standards and inconsistent conclusions are drawn depending on the analysts performing the review. A more consistent investigation approach requires detailed and prescriptive work instructions for the analysts to follow. This helps to drive a comprehensive investigation, a complete set of documentary evidence and a detailed rationale for the decision reached.

Guidance and training also need to be kept up to date, incorporating for example different typologies and case studies subsequently released by different regulatory bodies.

3. Use an appropriate workflow and alert management tool

A workflow tool is essentially a platform that allows analysts to manage all the procedures that they need to perform. We have seen workflow tools that are little more than spreadsheets with basic functionality and typically are not fit for purpose. A best in class transaction monitoring workflow tool should facilitate the assignment of alerts the right resources, provide all data needed for investigation (both internal and external) in one place and guide the investigator through a logical investigation process to ensure all factors are considered. It also provides a platform to store all additional information gathered during the investigation process. Use of such a tool allows management to enforce the guidance that has been provided to analysts and helps to ensure a consistent level of quality that would enable the financial institution to defend any decision taken about the alert in question in light of the evidence observed at the time of investigation.

[4] The STRO in Singapore, for example tracks the number of Requests for Assistance that it receives from overseas FIUs. For example: https://www.police.gov.sg/~/media/spf/files/cad/statistics/stro%20statistics%20-%20international%20cooperation%2020160915.pdf?la=en



Negative news screening is an investigative procedure that is generally poorly performed. Appropriate guidance, training and documentation of decisioning rationale are all critical to ensuring screening alerts are managed to a consistently high quality. The large volumes of alerts that are generated often include multiple duplicate articles, and often clearly irrelevant articles. The discounting of these articles distracts analysts from spending time considering potentially concerning articles.

Artificial intelligence tools are now available that can streamline the volume of articles requiring review from analysts. Traditionally, if analysts find 20 articles relevant to a party to the transaction, procedures require the analyst to read and review all 20 articles individually, even if they are essentially the same article. Instead of reviewing all of those articles individually, the artificial intelligence can determine that they all relate to the same story, which is only tangentially related to the question of financial crime. Provided an analyst reviews one of those articles, all 20 can then be reliably discounted as having no cause for concern. Such tools give analysts the opportunity to focus on assessing the real risk rather than performing duplicative tasks with limited value. Case study 2, outlined above ('When it goes wrong… insufficient and inexperienced staffing'), also highlights the importance of ensuring that analysts are supported by the right tools and systems to enable them to perform a proper job.

Post-investigation:
practice (and constructive feedback) makes perfect

Almost all of the institutions that we work with operate a level of quality assurance over their transaction monitoring, asking: “is the output of this process what it should be?”. Detailed checklists are an inevitable necessity to perform this process in a standardised manner. However, what is critical and often poorly executed is the feedback loop to remedy shortcomings identified in the quality assurance process. After all, what is the purpose of performing this assurance, if not to act upon any failings identified to ensure that they do not happen again? This can be performed at the transactional level or the process level, but also at the staff level. Management can use the output of their quality assurance processes to identify either specific staff that require further training or thematic areas that wider teams are struggling with and therefore broader remediation training is required.

In order to do so effectively, the information that management receives must be clear, concise and actionable as well as up-to-date and quantifiable. Too often, however, we find that management reporting information is the opposite. Done well, management information should provide a view of the process that allows management to take the right decisions and also impress upon staff the core purpose of their role of identifying suspicious transactions rather than just meeting operational targets.

Key response:

- Robust quality assurance framework
- Management information dashboards

Done poorly, management information can distort the facts, cause ill-informed decisions to be taken, or simply confuse the situation to the extent that management ignore what is presented.

Appropriate management information is key from a quality perspective, but also to help monitor operational efficiency. Good management information should provide actionable insights that flag risks of disproportionate work assignment, growing backlogs, underperforming teams or individuals and aged cases. Cross referencing this information with information on the quality of the team and individuals’ output provides a powerful tool for management to measure the impact of workload on quality.

Communication: just keep talking

Breaking down siloed operations is an important aspiration. Too often, one team will be working with little awareness or regard for what happens elsewhere in an organisation. From a transaction monitoring perspective, effective communication channels between functions are critical to maintaining adherence to regulatory expectations, while also ensuring that policy changes are practical and achievable. Moreover, good communication between transaction monitoring, Know-your-Customer teams, sanctions experts, fraud experts and business managers responsible for relationships with the customers is critical for the efficiency of investigations. A common shortcoming relates to how policy and resulting process changes are communicated between Compliance and Operations teams.

However, there are many permutations of poor communication. Communications with regulators is another channel that is often overlooked. Obtaining any necessary clarification, digesting any releases, case studies and typologies issued as well as providing regular and good quality Suspicious Transaction Reports is critical. The simple answer is to make sure everyone in the process just keeps talking.

Key response:

- Regular forums or committee meetings

Towards Better Transaction Monitoring

Effective alert handling is a critical step in the transaction monitoring programme. After all, what is the point of implementing systems to analyse transactions if the results of that monitoring are overlooked or not understood?

Financial institutions have been performing transaction monitoring as part of their anti-financial crime programmes for years, balancing how to ensure that they do not overlook suspicious transactions, whilst also avoiding casting the net so wide that unmanageable volumes of alerts are generated.

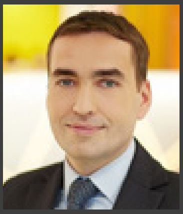
Recent developments in technology has rightly led to greater focus on the alert generation processes, with many organisations reviewing their platforms and tuning specific scenarios used to trigger alerts. However, whilst this is a key component, too often what happens after the alert generation is given a lower priority.

However, there are significant opportunities to deliver substantial efficiencies when the alert handling process is designed and executed effectively. At the moment, this is a largely manual process. However, there are areas that can be automated to boost efficiency. For those processes that are manual, ensuring that staff have the right training and the right information at their fingertips is critical. Getting alert handling right can save money for financial institutions and enhance their fight against financial crime.

Contact us

Richard Major

Partner, Financial Crime Unit,
South East Asia Risk Consulting Leader
PwC Singapore
+65 6236 3058
richard.j.major@pwc.com



Damian Kalinowski

Partner, Financial Crime Unit,
PwC Poland
+48 22 746 7197
damian.kalinowski@pwc.com

Nick Davison

Financial Crime Unit Leader,
South East Asia Consulting,
PwC Singapore
+65 9732 7330
nick.davison@pwc.com