AML Transaction Monitoring

A Survey of UK Financial Institutions

September 2014

Building a better working world

Contents

Executive summary

01

Transaction Monitoring (TM) is a critical, and resource intensive, component of an effective Anti-Money Laundering (AML) programme. In response to demand from UK Financial Institutions for an industry benchmark for TM we conducted a targeted survey to provide a snapshot of the current state of TM as well as plans for the future.

Our survey reveals that there is a large variation in how TM systems and controls are implemented, configured and managed. There appears to be a broad lifecycle of maturity that banks are following in their adoption of TM. Organisations earlier in the lifecycle are facing the challenge of how to improve their alert performance and adequately cover their AML risks; institutions that are further developed in their TM functions face the challenge of bringing operational costs under control.

This variation amongst institutions is most evident in the alert effectiveness rates achieved (in particular conversion of alerts to Suspicious Activity Reports) and the number of alert investigators employed to monitor a given number of accounts. There is a clear correlation between the level of satisfaction with TM and alert performance. However, there is no clear consensus as to what level of alert performance institutions should be aiming for.

The survey results show that there are significant variations in other areas. From a technology perspective, some institutions have a higher level of automation and sophistication across alert generation and case management than others. Similarly, some have much richer Management Information (MI) available than others. From an operational perspective, there are substantial differences in the way institutions have configured their vendor TM systems and the processes for ongoing alert tuning.

Survey Overview

EY conducted a targeted survey of AML Transaction Monitoring (TM) professionals in order to obtain a benchmark of the maturity of TM controls across the UK Financial Services Industry.

The 38 question survey comprised the following sections:

- Introduction and TM metrics (12 questions)
- Governance and management information (10 questions)
- Technology (9 questions)
- Alert coverage and quality (5 questions)
- Investigation management (2 questions)

The survey ran for several weeks in Q2 2014 following a TM round table event for UK banks.

Survey Participants

- The survey was targeted at compliance, operations and technology leaders involved in AML TM at UK banks.
- Respondents' roles included Money Laundering Reporting Officers, Heads of Financial Crime Compliance, Alert Investigation Managers and TM Systems Managers.
- Survey responses reflected different sectors within the banking industry including retail banking, corporate and wholesale banking, private wealth and securities brokerage.
- The survey was targeted at UK banks, but in many cases the responses reflected a global view across the organisation.

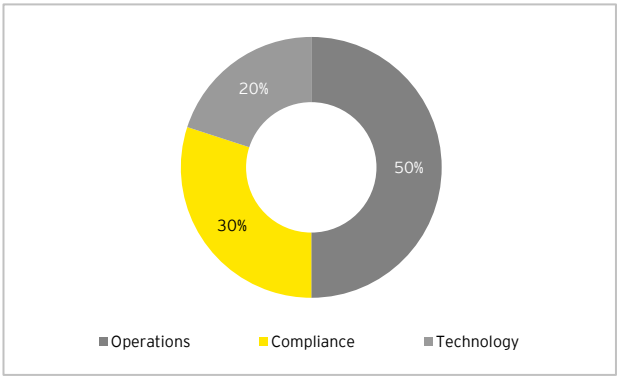

Figure 1: Distribution of respondents by role

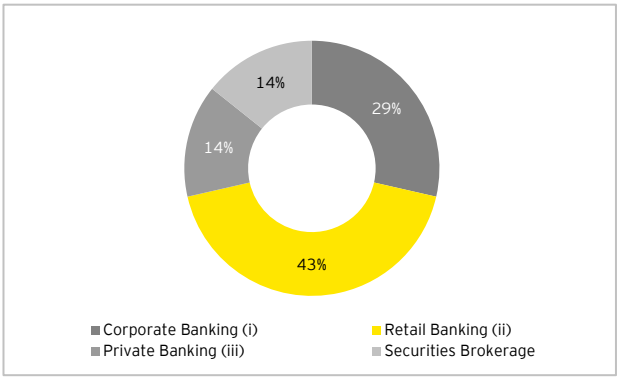

Figure 2: Distribution of respondents by industry sector

(i) Includes Corporate and Wholesale banking
(ii) Includes Retail Banking, Credit Cards, Small/Medium Business Banking and Retail lending services
(iii) Includes Private Banking and Wealth Management Services

General findings

02

There is a wide variation in both the number of automated TM alerts that banks generate and the operational cost of investigation.

Our survey covered a wide range of regional and global banking operations, from a division monitoring 5,000 accounts to global banking operations monitoring over 100 million accounts. As expected, different sizes of TM operation generate different numbers of monthly alerts. What is surprising is the large variation in the number of alerts generated on average per alert investigator, i.e. when you normalise the data. This reflects a large variation in the operational cost of a TM function: even amongst institutions with similar business profiles, some have 20 times more alerts generated per alert investigator than others.

There is an even wider variation in the alert generation rates per account, especially when looking across all business lines.

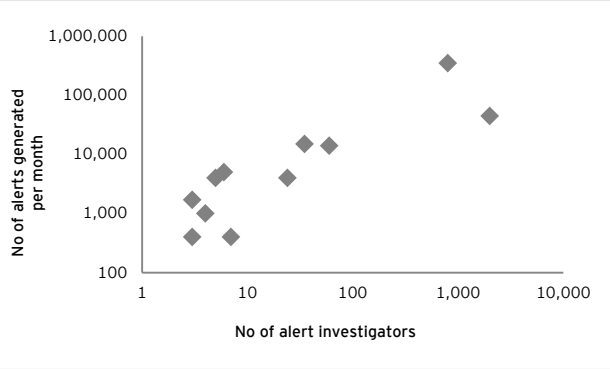

Figure 3: Number of alert investigators vs. number of alerts per month

Approximate number of alerts per alert investigator per month

Average	Maximum	Minimum
357	833	22

Approximate number of accounts per alert investigator

Average	Maximum	Minimum
1,506,102	8,333,333	143

There is a large variation in the effectiveness of alerts generated by automated TM systems, particularly across different sectors.

Typically the Retail Banking sector achieves the best conversion rates of alerts into Suspicious Activity Reports (SARs) – up to 20% in some cases – and the best overall rates of alerts worthy of investigation – as high as 90% in some instances. At the other end of the spectrum, Securities Brokerage and Corporate Banking businesses have SAR conversion rates as low as 1% and alerts worthy of investigation as low as 5%. Whilst some of this variation may be attributable to differing policies as to when to file a SAR and as to what constitutes a worthy alert, it is notable that institutions with higher alert performance rates register higher satisfaction ratings with their TM technology and overall TM programmes.

The differences in alert performance appear to not be correlated with the underlying systems used or with the individual scenarios configured within those systems – in other words, all vendor systems were considered effective at detecting activity worthy of investigation. Rather, the level of maturity of the alert investigation organisation and governance around the TM function seems to be a factor. But the most significant factor is likely to be the nature of the business itself: suspicious activity is easier to identify in the Retail Banking sector where customer behaviour more naturally falls into well-defined segments.

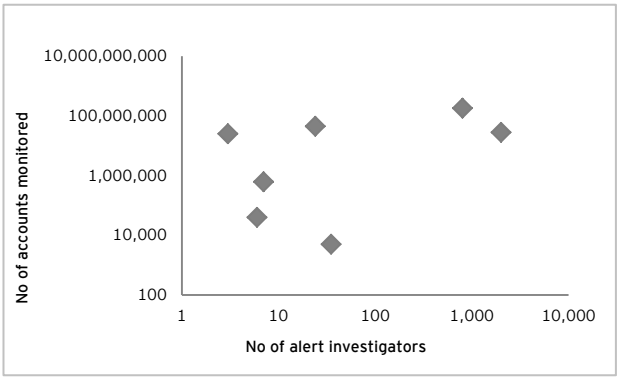

Figure 4: Number of alert investigators vs. number of accounts

02 General findings

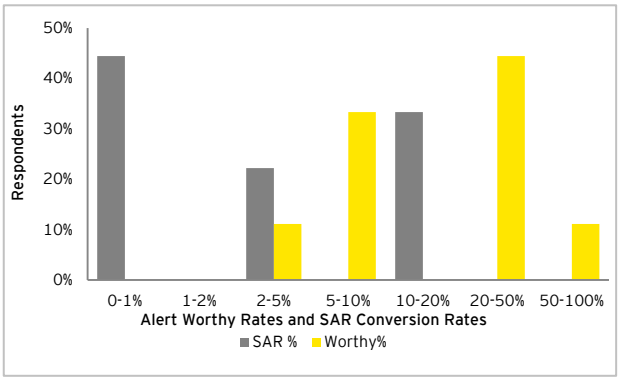

Figure 5: Percentage of worthy alerts vs. SAR rates

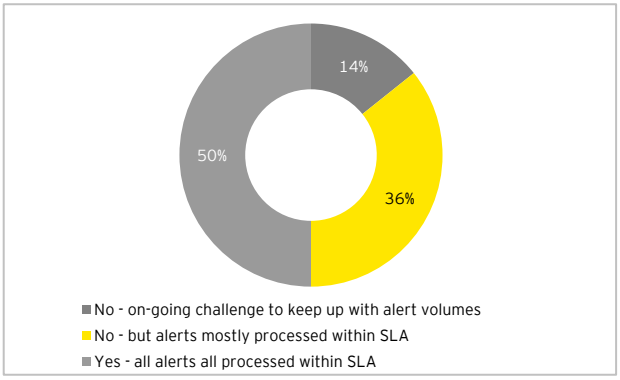

Figure 6: Are your alerts investigated in a timely manner?

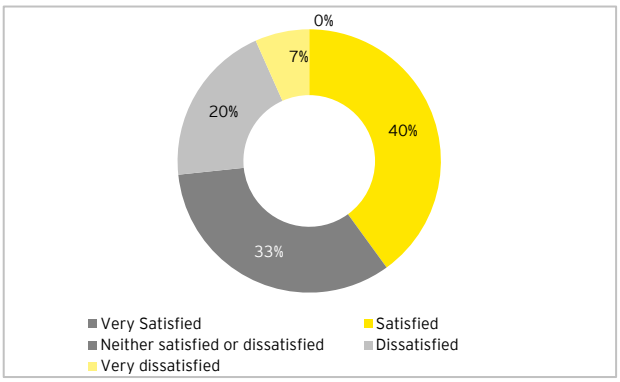

Figure 7: How satisfied are you with the overall effectiveness and value of your Transaction Monitoring (TM) solution(s)?

Alert effectiveness and operational expenditure correlate with maturity of Management Information (MI), technology implementation and alert investigation

We see a correlation between overall alert performance and associated operational expenditure on alert investigation and the level of maturity of the TM organisation in other areas. For example, more sophisticated institutions tend to have their alert investigation more specialised by business line rather than relying on a single shared service model.

Similarly, institutions with better alert performance tend to have more sophisticated MI, for example tracking operational efficiency, data quality and system performance in addition to basic alert metrics

From a technology perspective, more mature institutions tend to have all accounts monitored by a single TM system, but with multiple instances across different business lines and geographies.

Financial Institutions rely on both automated TM and manual alert generation

Despite the sophistication of automated TM solutions, nearly all institutions still process significant volumes of manually generated alerts. Assuming manual alerts are of higher 'quality' than automatically generated alerts, there is an opportunity to feedback learnings from manual alerts into the configuration of the TM systems.

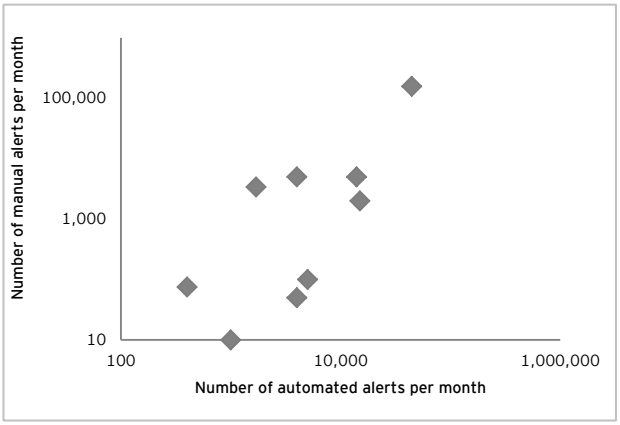

Figure 8: Number of automated alerts vs. number of manual alerts

Financial Institutions know they need to do more, but what this means is unclear

Financial Institutions want to do more with their TM programmes. For institutions with poor alert conversion rates, this means getting more out of their technology and evolving their operational processes. For institutions that already have TM programmes with which they are broadly satisfied, the focus is more on reducing operational expenditure.

In summary the bar for TM and what constitutes "good" is unclear. Respondents indicated that investment in TM is seen as harder to justify than sanctions screening, where the results may be seen as more binary, and that TM deployments even within the same organisation can vary significantly in their effectiveness.

Governance 03

Very few institutions implement a dedicated strategy for TM, rather it is part of a broader AML or Financial Crime strategy.

When surveyed on TM strategy, respondents were evenly split between those that included their TM strategy within an AML strategy and those which included their strategy as part of a wider approach to financial crime.

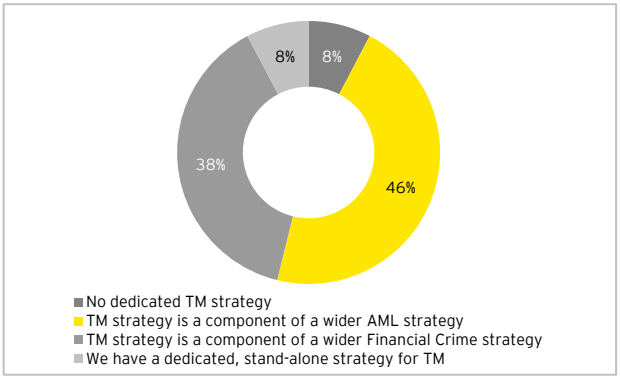

Figure 9: Which of the following describe the TM strategy in your organisation?

However, few institutions are considering synergies with other areas of financial crime in their strategies, such as fraud and tax evasion.

With regards to the content of TM strategies most frequently cited were initiatives to upgrade technology platforms. The exploitation of synergies with other areas of financial crime was the least mentioned initiative – this could be considered contradictory considering that a significant volume of institutions have a TM strategy that is part of a wider approach to financial crime.

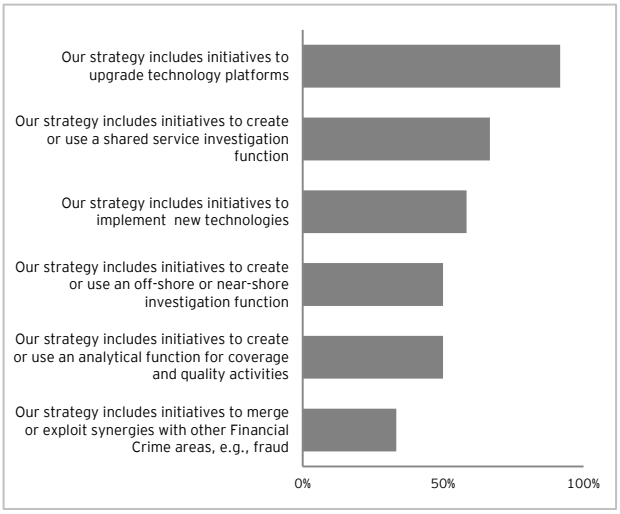

Figure 10: Which of the following initiatives are contained within your TM strategy (select all that apply)?

Only a minority of institutions surveyed feel that they have comprehensive coverage in all areas of their TM policy.

Over half of respondents acknowledged that they have gaps in the implementation of their TM policy that need to be addressed. Most respondents indicated that a separate TM policy is in place for each business line or region and some implemented an enterprise wide TM policy. Specific feedback in this area indicated that a policy emphasising a consistent minimum standard with local augmentations was the objective of most institutions.

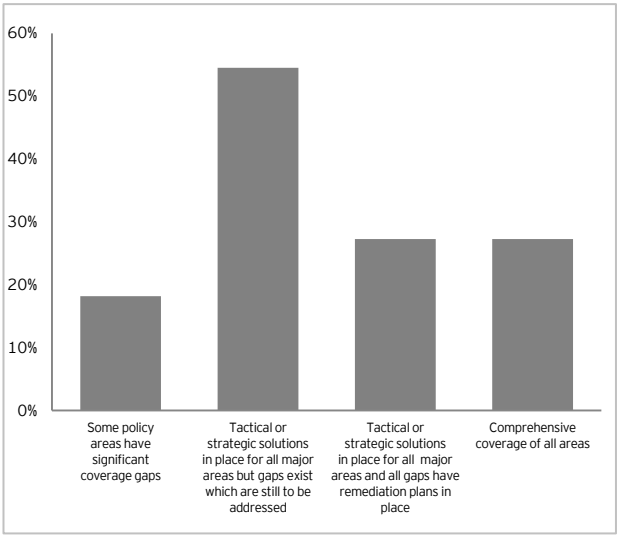

Figure 11: How fully implemented is your TM policy (select all that apply)?

The majority of respondents utilise a shared service function to process TM output; however, few share this information with an FIU (Financial Intelligence Unit)

With respect to institutions' operating models two-thirds of respondents indicated that they use a shared service model crossing multiple regions and lines of business. However, there were still significant responses that indicated siloed business line models. These responses were commonly mentioned in the context of providing specialist investigation services for areas such as correspondent banking and trade finance. A small number indicated that they used a shared model interfacing to an FIU for information sharing. This approach is seen as the one that most institutions are inclined to move towards.

03 Governance

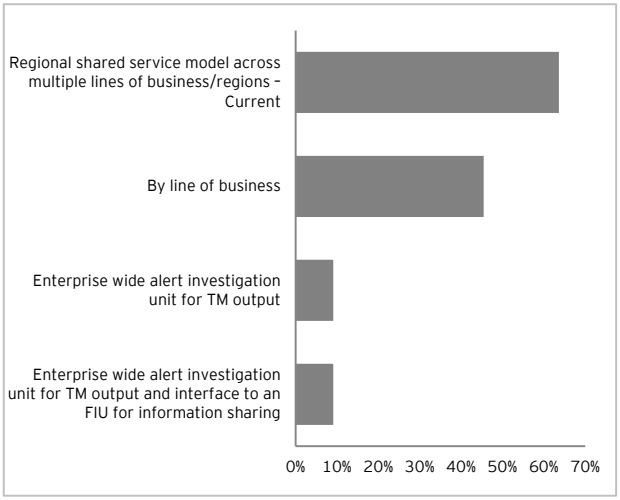

Figure 12: How is the TM operating model defined within your organisation (select all that apply)?

The level of satisfaction toward MI is mixed, with institutions more satisfied by richer information covering not only alerting volumes, but, coverage, effectiveness and operational metrics.

The satisfaction toward MI is mixed amongst respondents. Responses appear to be correlated to the amount of information that is available – the broader number of metrics the greater satisfaction that is expressed. Areas for future consideration are focused in data quality and technical performance for most institutions. Only around 60% of respondents' current capabilities measure alert effectiveness and less than 40% capture MI on data quality.

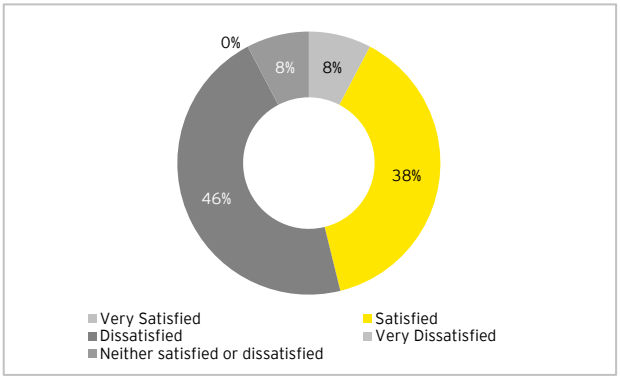

Figure 13: How satisfied are you with the overall effectiveness of your TM MI?

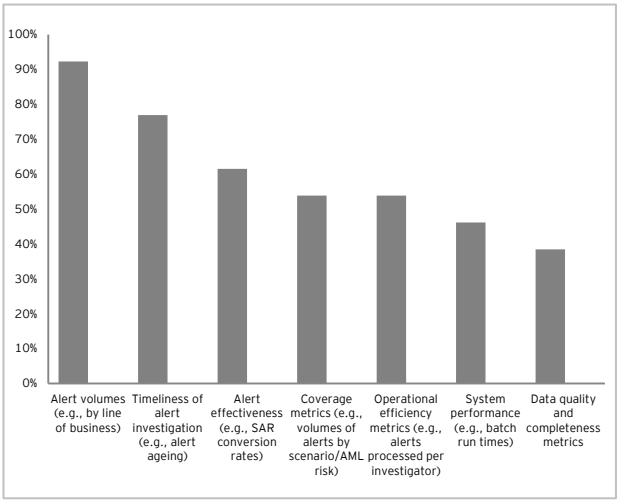

Figure 14: What MI do you currently produce relating to TM (select all that apply)?

Most institutions have semi-manual MI but are moving towards more automated MI production.

The majority of institutions use a combination of reports generated using their TM platform which is supplemented with semi-manual processes. Usage of dedicated MI tools is limited with provision of interactive reporting even less prevalent. Institutions are however moving toward an environment where dedicated MI capabilities are used to a greater degree with a number mentioning a planned transition in the next 1 to 2 years.

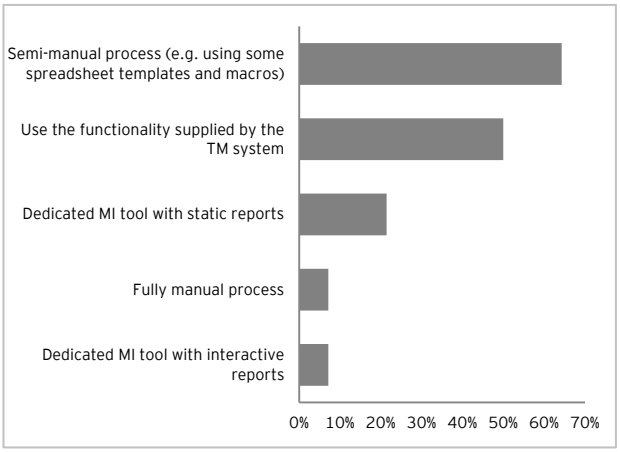

Figure 15: What level of automation do you have for your TM MI (select all that apply)?

Technology 04

Institutions have typically deployed multiple instances of automated TM platforms across businesses and regions.

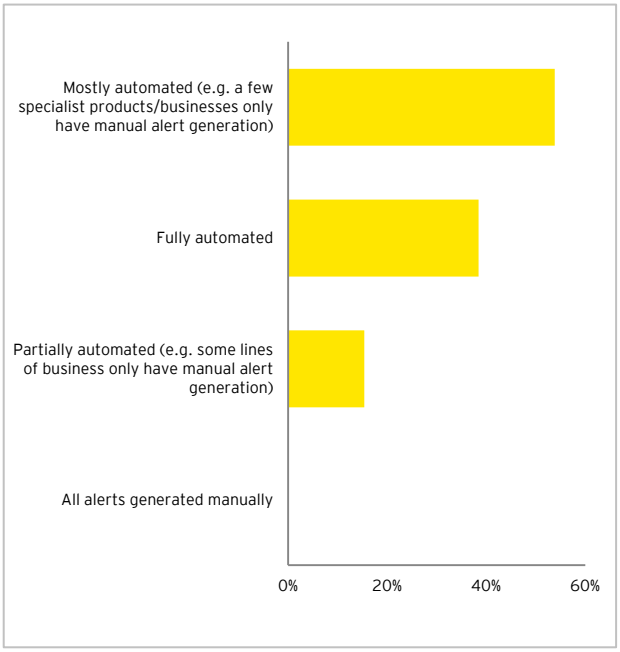

Figure 16: What level of automation do you have for your TM alert generation (select all that apply)?

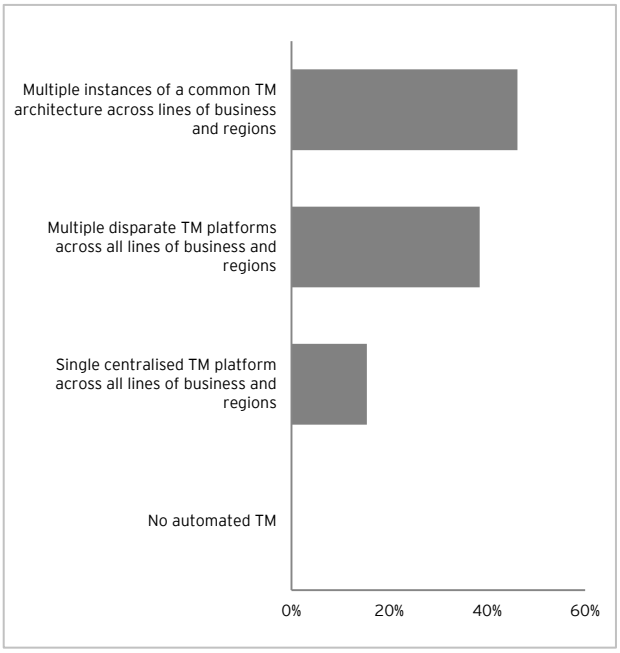

Figure 17: Which of the following describe the use of TM software in your organisation (select all that apply)?

Respondents use a variety of vendor supplied TM systems.

NICE Actimize (Monitor and Suspicious Activity Monitor (SAM) and Oracle (Mantas) are the most widely used TM vendors in our sample, with the majority of respondents either currently having these products installed in some part of their organisation or planning to implement them in the next 12 to 24 months. Note that some respondents utilise more than one TM vendor in their technology landscapes.

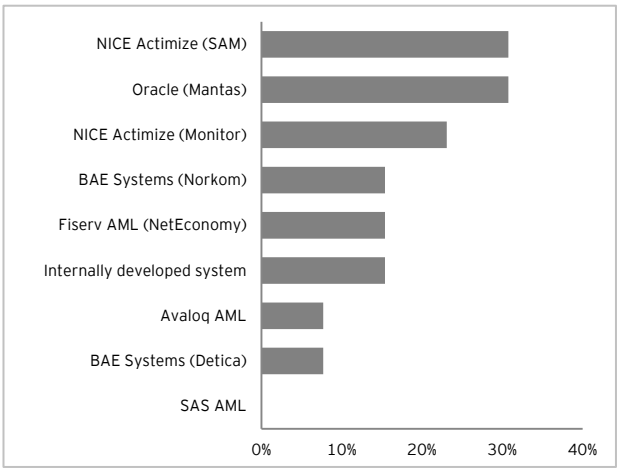

Figure 18: What vendor TM systems do you use (select all that apply)?

Satisfaction levels on the overall effectiveness of TM software varied amongst respondents with more than half expecting more from their existing platforms.

Overall TM satisfaction varied and is generally correlated with the alert conversion rates discussed in the General Findings section.

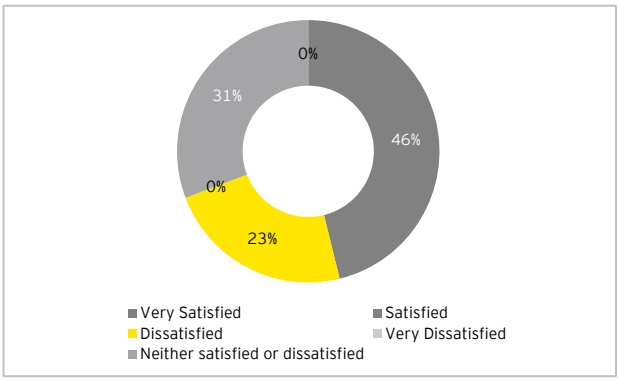

Figure 19: How satisfied are you with the overall effectiveness of your TM software?

04 Technology

Data transformation processing across institutions is quite similar with transaction data being directly extracted from source system and prepared in a staging area prior to being ingested in the TM platform.

Over two-thirds of the respondents had a similar approach to data management by extracting data from source systems into an Extract, Transform and Load (ETL) platform before being ingested into the TM software.

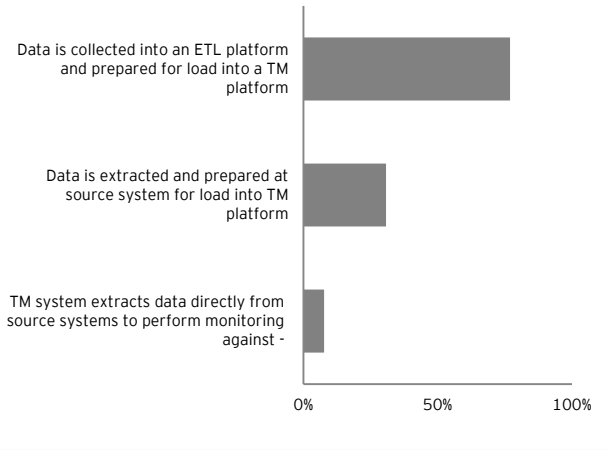

Figure 20: How is data obtained for your TM system(s) (select all that apply)?

Institutions do not rely on a single control mechanism to monitor the quality and completeness of data being ingested into the TM software; instead they typically use a combination of ad hoc checks around a dedicated programme level data quality review.

When surveyed on the approach towards data quality and completeness the results were quite evenly distributed amongst respondents, with a combination of ad hoc checks, periodic data quality reviews, file level reconciliation and sample based checks.

There appears, however, to be a correlation between the sophistication of data quality controls, the completeness of MI and overall satisfaction with TM. Similarly, institutions with good MI and data quality also typically have better alert performance.

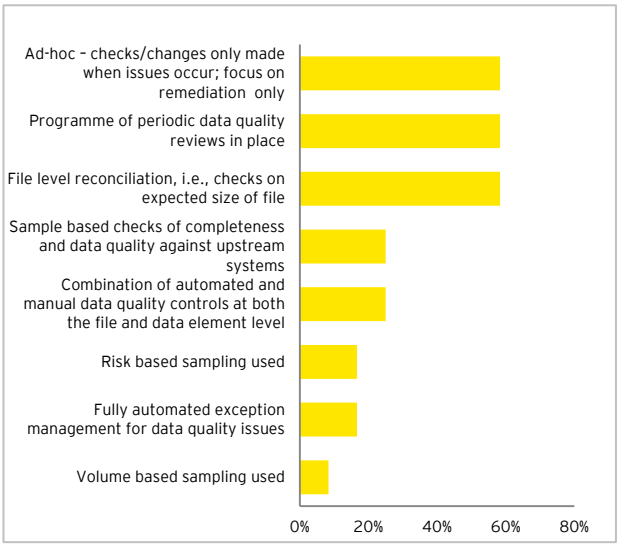

Figure 21: Which of the following describe the processes for ensuring good quality data in your TM system(s) (select all that apply)?

The majority of respondents have TM alert data fed into their investigation platform or have provided access to alert data from the source systems.

When queried on how they would describe their investigation platforms for AML alerts, half of respondents described conducting manual investigations. Other responses were extremely mixed with less than a third utilising a centralised or integrated case investigation platform. There exists a high incidence of varied platforms used across divisions and geographies.

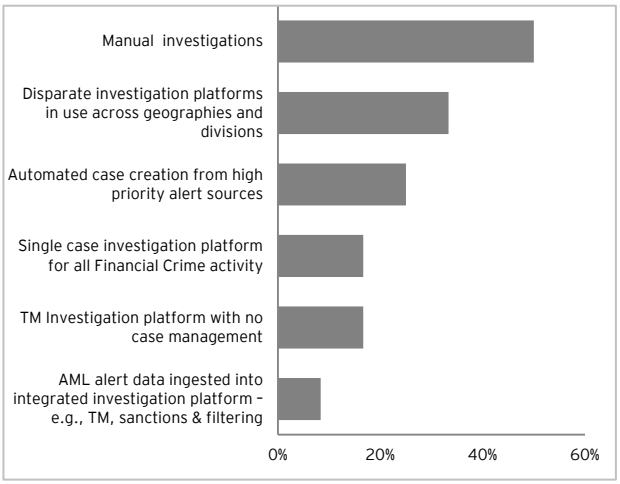

Figure 22: Which of the following describe your investigation platform for AML alerts (select all that apply)?

With respect to data availability most respondents relied on the data ingested into their relevant TM or specific investigation platform. A minority have the more advanced capability to link their analysis to other relevant AML systems and a similar minority rely on just using references to link cases with relevant data.

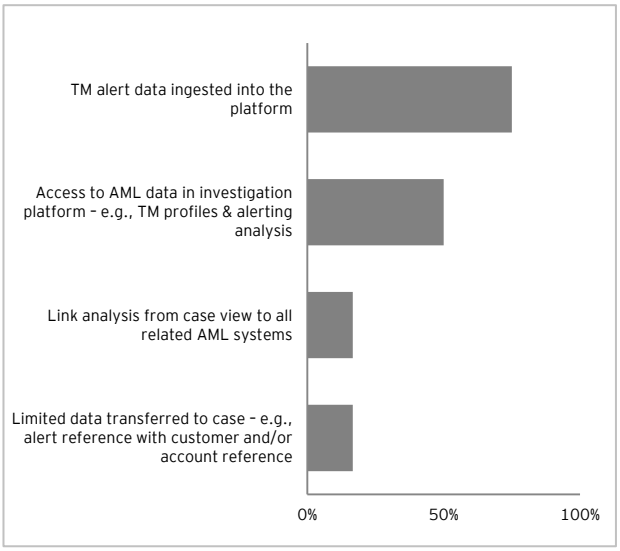

Figure 23: What data is available on your investigation platform (select all that apply)?

Almost all institutions described having a multi-level investigation workflow, with some configured by geography and half of respondents enabling a restricted workflow for specific customer types – such as employees and sensitive customers.

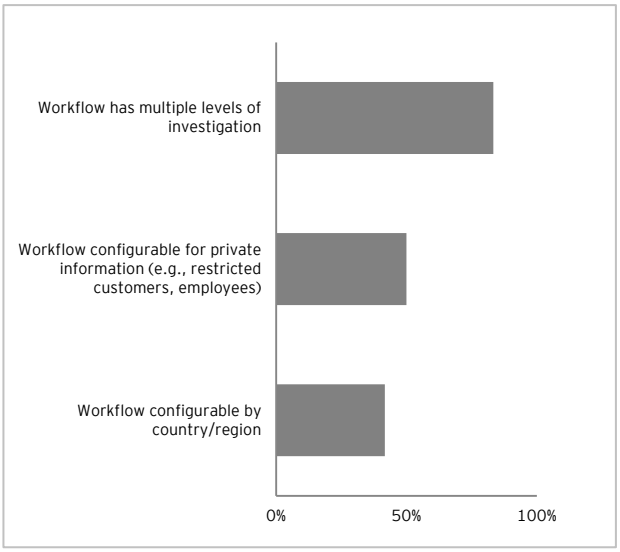

Figure 24: Which of the following describe the workflow on your investigation platform (select all that apply)?

Coverage and quality

05

Although all respondents are using vendor built scenarios, the majority feel these only partially met their monitoring needs.

When queried about their software vendor purchased monitoring systems only a small minority of respondents felt that that the provided scenarios were very robust.

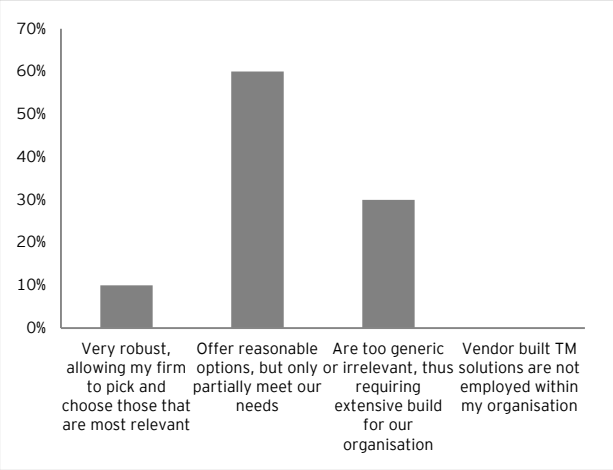

Figure 25: Which of the following best describes the scenarios provided with vendor purchased TM systems?

Use of alerting entities such as social networks and groups of connected entities is limited with transactions, accounts and customers remaining the key alerting entities in TM. Of developing interest however, is alerting against the customer's customer being the most popular alerted entity to be planned in the next 12 to 24 months.

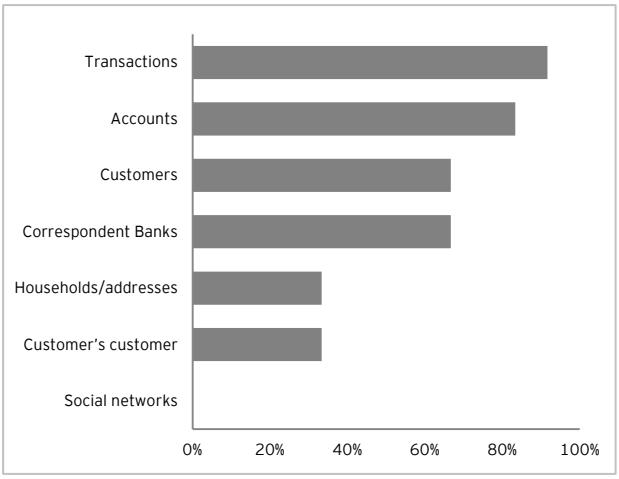

Figure 26: Which of the following describe the 'entities' that your TM system monitors or alerts on (select all that apply)?

There is a fairly consistent set of TM scenarios used across most institutions. Rapid movement of funds and large value/volume transaction pattern scenarios are pervasive across all respondents.

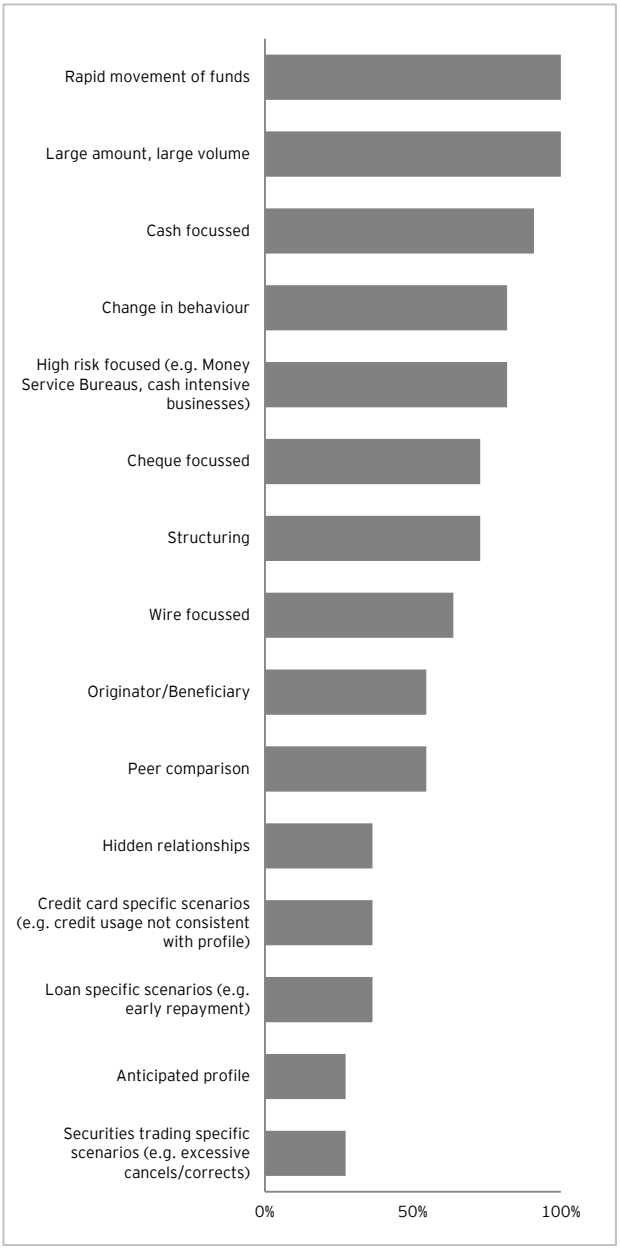

Figure 27: Which of the following scenarios do you use in your TM platform (select all that apply)?

05 Coverage and quality

Many institutions are planning to build a dedicated analytics team, utilising formalised scenario libraries with a rapid development capability

Most institutions are yet to implement a standardised approach although many have a more advanced approach to tuning planned in the next 12 to 24 months. Additionally, current analytical techniques are limited with most relying on historical data to tune for coverage and alert volumes.

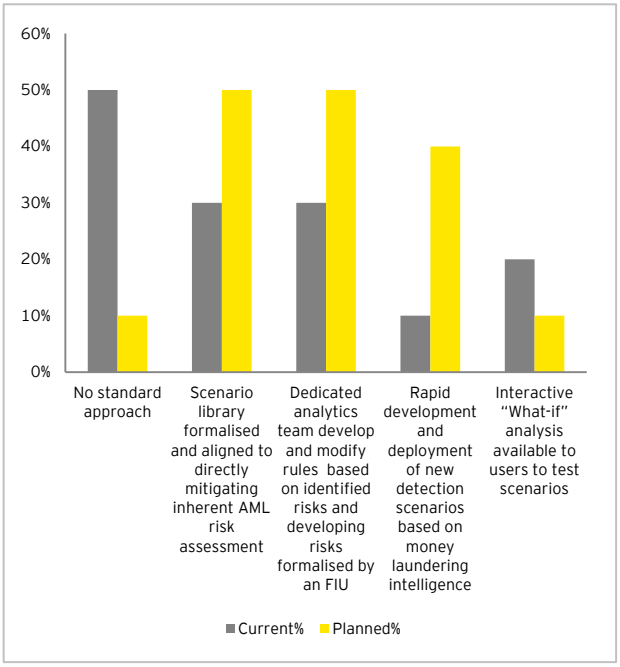

Figure 28: How are your TM scenarios developed and maintained (select all that apply)?

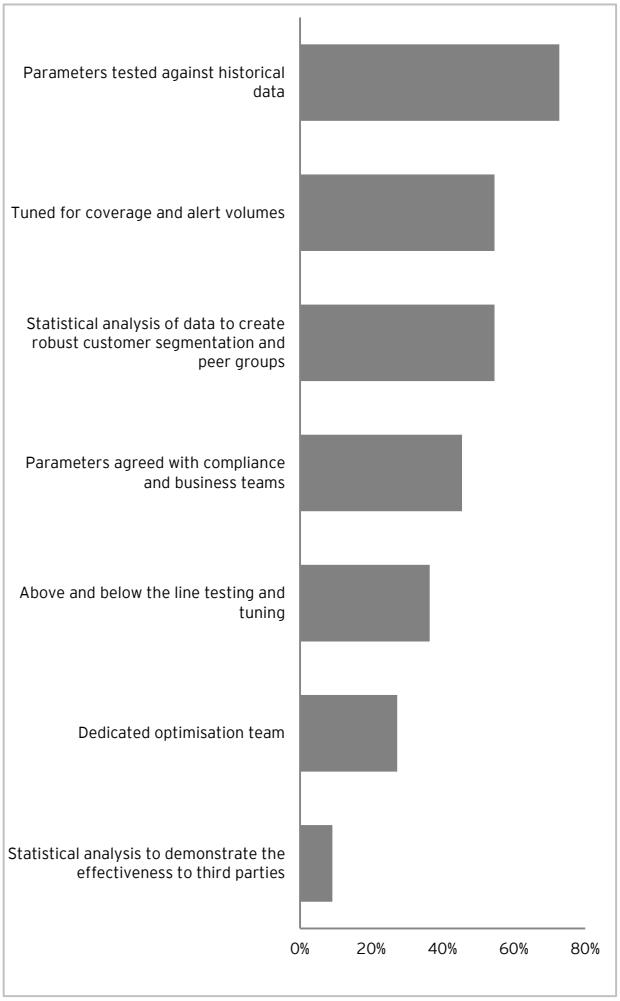

Figure 29: How are your TM scenarios tuned (select all that apply)?

Investigation management

06

The alert investigation process is generally consistent across institutions

The majority of institutions surveyed have a separation of duties in alert investigations between level 1 and level 2 teams to ensure obvious false positives are discarded and only worthy alerts are reviewed for further analysis.

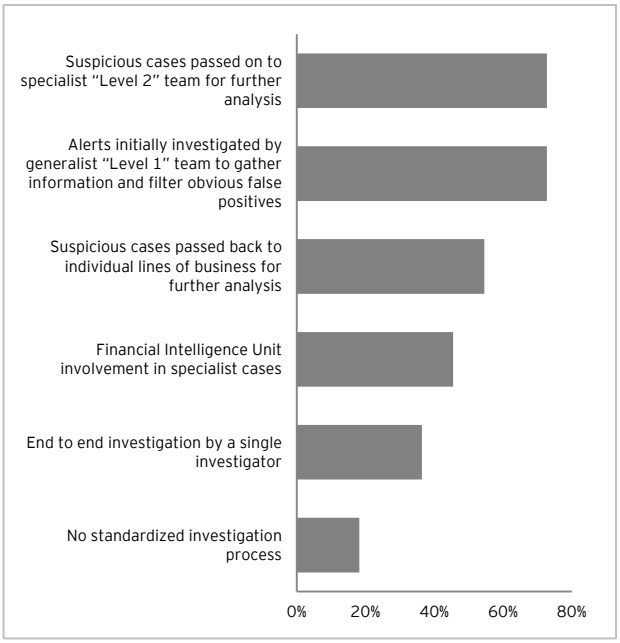

Figure 30: Which of the following best describe your investigation process/workflow (select all that apply)?

Only half of institutions use automated SAR filing

50% of the institutions surveyed use automated SAR filing. The reason this figure is not higher may be due to the relatively low SAR conversion rates experienced by many organisations as mentioned earlier in the general findings section.

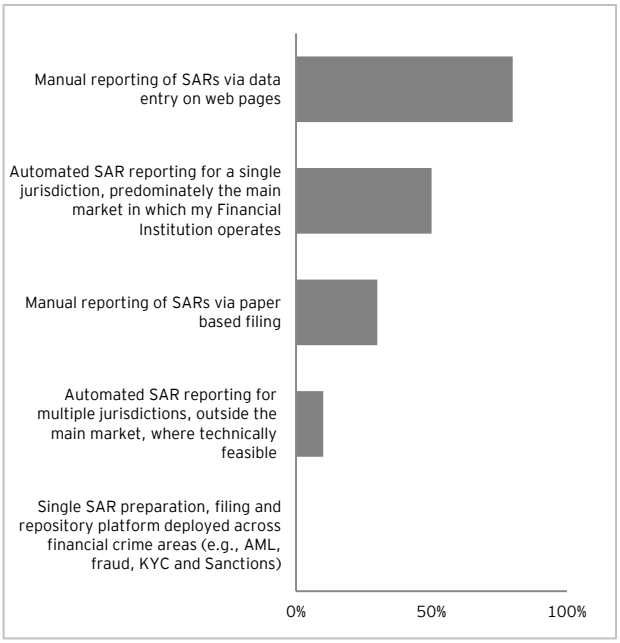

Figure 31: How are Suspicious Activity Reports (SARs) filed within your business line (select all that apply)?

Conclusion – a lifecycle of maturity

07

Financial institutions face common fundamental challenges in AML Transaction Monitoring of keeping operational costs under control whilst ensuring adequate mitigation of money laundering risk. The survey results support the view that many organisations follow a common lifecycle of maturity in addressing these challenges.

We see six discrete stages aligned to the management of risks and the control of operational costs. These are summarised below.

Stage 1 – Introducing an AML TM solution. The first stage of maturity is simply the implementation of an automated TM solution where previously one did not exist. This provides a minimal level of risk management with an initial, increasing operational cost.

Stage 2 – Stabilisation of an AML TM platform. As a result of lessons learnt from the initial solution implementation institutions are able to achieve efficiencies and balance a basic level of cost and risk.

Stage 3 – Improved coverage of AML risks. Pressure from regulators and internal control functions demand that TM provide better coverage of AML risks, but this comes at a significant increase in technology and operational cost as system coverage is extended, new rules are added and thresholds are lowered.

Stage 4 – Rationalisation. Refinements in operational processes and systems management, and more effective application of analytical tools and methods drives decreases in costs and further decreases in residual AML risk.

Stage 5 – Steady state. Mature governance, MI and a dedicated TM analytics function ensures new threats are addressed effectively whilst keeping operational costs under control.

Stage 6 – High performance AML function. Leading edge technologies and investigative processes are applied on an opportunistic basis to drive further cost reduction and improved risk management.

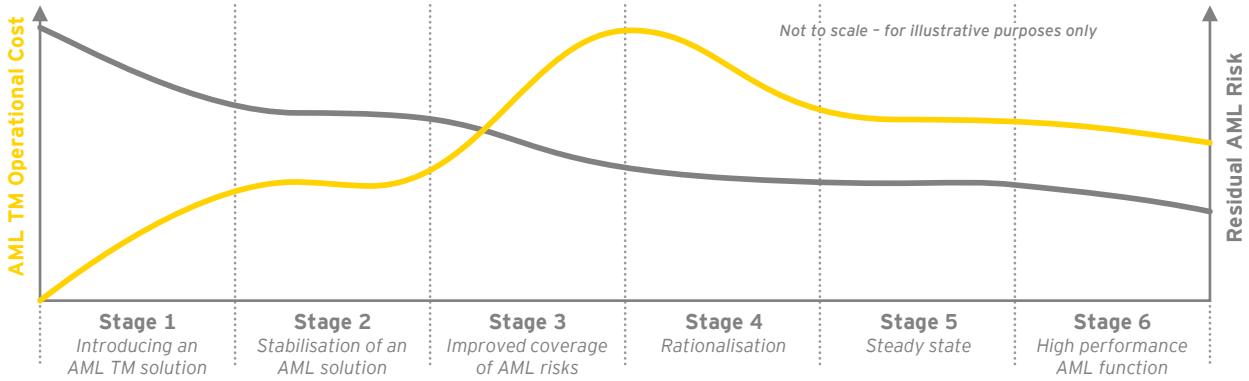

Figure 32: The relative relationship of operational costs and residual risks in Transaction Monitoring across the stages of maturity.

From our survey it appears that many UK Financial Institutions in are aligned to Stages 2 and 3 with a smaller number in Stage 4 in the maturity model. The challenge for institutions that are in the earlier stages of the model is to avoid the impending rapid increase in operational cost that will likely result from regulatory pressure to drive down risks. For institutions that are more progressed, their challenge in Stage 4 is to quickly reduce the already high operational costs caused by increased alert volumes and large investigation operations.

For institutions considering how to further control their AML risk, the approach is not as simple as increasing the depth of coverage, as this will drive increases in alert volumes and consequently investigation operations. A more sustainable response appears to be for institutions to enhance their fundamental capabilities in TM, by investing in:

- Strategy, policies and governance that drive consistent approaches to technology and operations, where necessary highlighting requirements for specialist monitoring situations
- Regular MI not only on aggregate output of monitoring scenarios, but on the quality and completeness of data ingested into the system, and effectiveness of investigations
- Analytical functions that are able to optimise coverage with evidenced results and respond to new threats with rapidly developed scenarios and controls
- Smarter operational management with specialized teams, a risk focused approach and better defined processes and procedures

Contact information

08

Contact information

Patrick Craig
Partner, Financial Services Advisory

pcraig@uk.ey.com
+44 20 7951 9999

Debbie Ward
Partner, Financial Services Advisory

dward1@uk.ey.com
+44 20 7951 1134

Jodie Forbes
Senior Manager, Financial Services Advisory

jforbes1@uk.ey.com
+44 20 7783 0744

Matt Reed
Senior Manager, Financial Services Advisory

mreed@uk.ey.com
+44 20 7951 7870

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP

The UK firm Ernst & Young LLP is a limited liability partnership registered in England and Wales with registered number OC300001 and is a member firm of Ernst & Young Global Limited.

Ernst & Young LLP, 1 More London Place, London, SE1 2AF.

ED NONE

1488612 (UK) 09/14. Creative Services Group.

In line with EY's commitment to minimise its impact on the environment, this document has been printed on paper with a high recycled content.

ey.com/uk