



---

**Author**



**Richard Major**  
richard.j.major@sg.pwc.com  
Partner  
+65 9117 7740

---

# From defective, to detection: How to improve your transaction monitoring system

**The detection of suspicious activity through effective Transaction Monitoring (TM) systems is a key control in the management of money laundering and terrorism financing (ML/TF) risk.**

**Financial institutions face several common challenges in the design and ongoing maintenance of TM systems, including the ability to analyse complex data and operational inefficiencies created through large volumes of false positive transaction alerts. Throw in several high profile enforcement actions<sup>1</sup> that included Transaction Monitoring control weaknesses and financial institutions have never been under more pressure to get this right.**

**Here's some practical solutions to each of the common challenges.**



## **Maintaining an effective transaction monitoring system**

Ensuring transaction scenarios and thresholds are appropriately calibrated on an ongoing basis is particularly challenging. This is compounded by the scarcity of employees with the necessary technical data management and analytical skills required to conduct effective assessments and refinements of the systems.

Data accuracy and completeness is also a crucial part of the ongoing effectiveness of Transaction Monitoring. This includes the interaction with upstream and downstream applications, such as core banking platforms, case management systems and management information systems.

Put simply - have you assessed that all applicable products and services are finding their way to the appropriate system rules and scenarios and is there accurate and complete information contained within any reports that will be extracted for reporting purposes?



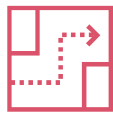
## **Effective investigations**

Another common challenge is ensuring the quality, accuracy and consistency of the handling of alerts generated from TM systems. The need for a properly defined, documented and consistent investigative process to resolve alerts would seem self-evident, but it is surprising how often financial institutions overlook the need to invest in both their capability and capacity in this area.

As a starting point, financial institutions should ensure that staff involved in the review of Transaction Monitoring alerts are adequately skilled and experienced to identify and assess suspicious activity and make appropriate decisions for escalation or reporting.

This can be achieved partly through specifying a list of minimum standards required when investigating an alert, such as requiring the analyst to document their comparison of triggered transactions against the expected activity identified in the KYC profile. An analyst's documentation of their investigation should also address the ML/TF typology triggered - a well mapped and risk-based calibrated TM system will allow the analyst to target the typology that the triggered scenario(s) is designed to pick up.

With minimum standards of investigation established, financial institutions may consider implementing scorecards to gauge the completeness and accuracy of investigations conducted on each alert. Detailed management information and trend analysis on these scorecards can measure quality at an individual or functional level, inform targeted training needs by individual or topic and measure the effectiveness of any training delivered.



### Developing a strong AML/CFT culture

The best controls and processes still require an appropriate mind-set in the employees who are charged with executing them. Financial institutions need to constantly train, monitor, identify weaknesses, remediate, and re-monitor to raise risk awareness and develop a strong AML/CFT culture throughout the institution.

A practical means of achieving this can be through an effective, independent, quality assurance (QA) programme as part of the first line of defence. For a QA programme to be effective, it should be sufficiently independent, having appropriate reporting lines to escalate issues. It should also be risk focused, varying the frequency and intensity of monitoring to the level of risk identified. This allows timely identification of weaknesses, proper understanding of cause (e.g. lack of training, process failure, individual error), and effective remediation.

A mature QA loop can promote the desired AML/CFT mind-set and ethical standards among employees. Whilst more resources may be required at the initial phase to change existing processes and mind-set, the constant feedback, senior management attention, and focus on high risk areas can eventually mature to significant exception based reporting, enhancing the continuous improvement of the Transaction Monitoring framework.



### Effective senior management oversight

The reporting and escalation of significant risk matters to senior management should be considered, including reporting Transaction Monitoring statistics on the quality and timeliness of alerts, such as ageing statistics with pre-determined risk levels.

By way of example, where management's risk appetite for the clearance of alerts is 20 days from the alert generation date, an unresolved alert age of 15-19 days may not yet be an operational failure, but will represent an increased risk of exceeding the pre-determined 20 days, and hence pre-determined risk appetite.

An effective management reporting framework will provide senior management with timely and actionable information, allowing

proactive adjustments to be made before risks become issues. It will also assist in the development of a strong AML/CFT culture across the financial institution and ensure that the TM system is not a 'set and forget' process.



### Outsourcing

Good governance and strong oversight of any outsourced function is required to ensure that the outsourced service provider (OSP) performs the service to the standards required by the financial institutions policies and procedures.

The selection of an OSP that is involved in any aspect of the TM system should place strong emphasis on the OSP's entity level controls, information technology and service level controls. Prior to outsourcing, it is also critical that the financial institution has developed well calibrated risk based scenarios that are tailored for the financial institution and not an 'off the shelf' set of rules.

Strong policies and procedures on the handling of alerts should also be documented, as well as a QA programme that is capable of identifying weaknesses in the functions being outsourced. An effective management reporting framework should also be established to provide senior management with effective oversight of the outsourced function.

With robust controls and governance, outsourcing has the potential to bring about material cost reductions, increased efficiency and more effective identification of suspicious activity. Most importantly, it can free up the highly skilled and often scarce financial crime and compliance resources, enabling them to focus on higher risk transactions and activities.

---

### Conclusion

**Significant regulatory scrutiny and the ever increasing sophistication of criminal techniques used to facilitate financial crimes creates additional pressures on financial institutions to maintain and enhance TM systems in order to prevent, detect and report suspicious activity as it occurs. An effective, end-to-end Transaction Monitoring framework is vital in achieving this.**

**A comprehensive, end-to-end approach that uplifts systems and technology but also promotes the better use of resource time are all crucial parts in the overall effectiveness of any TM system.**