

Misys Suspicious Activity Monitoring

Improve the efficiency and performance of your compliance effort

All financial services organisations around the world are now primary targets for a far tougher regime of global regulatory scrutiny, as regulators increasingly identify and respond to changes introduced by new, far reaching Anti Money Laundering (AML) and Countering the Financing of Terrorism (CFT) controls.

These changes, driven by regulation such as the 3rd EU Money Laundering Directive, Financial Action Task Force (FATF) responses and US Patriot Act, represent significant challenges for financial institutions all over the world.

Moreover, the escalating cost of compliance was highlighted by KPMG's Global Anti-Money Laundering Survey 2007. The costs of AML compliance have proved to far exceed expectations, with an estimated 58% increase since 2004.

One of the key trends to emerge from the new regulation is for banks to achieve an almost 'holistic' knowledge of each client's financial activities. Banks are often unable to take action using information from just one source, such as sanction lists. To get a more complete picture, Compliance Managers or Money Laundering Reporting Officers need a 24/7 understanding of customers' financial activity, based on close transaction monitoring.

Automated transaction monitoring

Automated transaction monitoring systems review thousands, if not millions, of transactions, enabling banks to undertake a daily risk-based analysis of each client's financial activities.

In this way, banks are in a much better position to identify and report potential money laundering or terrorist financing activity, thereby protecting themselves and their customers.

The Misys Suspicious Activity Monitoring (SAM) solution, delivered in partnership with Northland Solutions, enables banks to adopt this risk-based, automated approach to transaction monitoring. The system reduces the amount of time spent by analyst teams on manually monitoring and identifying suspicious activity, whilst supporting best practice compliance procedures.

Benefits at-a-glance

- + Pre-interfaced to Midas version 4.01, Midas Plus, Equation version 3.81 and above, and Bankmaster version 7.0
- + Detection rules are both risk weighted and can have multi-dimensional enabling banks to adopt risk based approach, whilst reducing the number of false positives
- + Rules Sets aligned to your banking sector can be licenced as separate modules, to ensure cost effectiveness
- + Sophisticated investigation workflow manages each exception in an intuitive way
- + Single point of information for all investigation notes and contacts, including liaison with your Financial Intelligence Unit (FIU) and other third party organisations
- + Built-in reporting functionality provides consolidated management information
- + A proven solution live at over 60 sites in 25 countries
- + Quick to implement, typically taking two months due to pre-integration with Misys applications (compared to normal 6-9 months)
- + Low system management overhead
- + Ongoing maintenance and updated Rule Sets to meet changes in the regulatory landscape

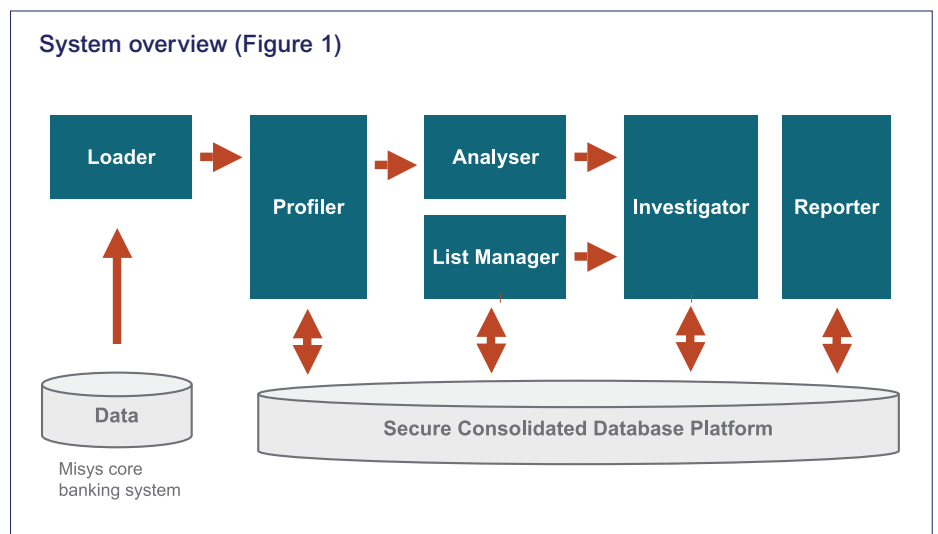
“Estimated money laundering flows are reported to be in excess of US\$1 trillion being laundered every year by drug dealers, arms traffickers and other criminals.”

Solution overview

The SAM solution provides two key elements: a risk weighted rules-driven process that identifies potentially suspicious activity; and a fully audited framework for case investigation and management.

As a proven solution live in over 60 sites in 25 countries, SAM is robust, innovative and quick to deploy. It is also easy for the users to understand, thereby delivering immediate efficiency gains to an organisation.

The SAM solution consists of a number of individual components, as outlined in Figure 1. These are described in more detail below:



- + **Loader** seamlessly and efficiently integrates the core data held in your Misys banking system. This delivers a consolidated view of the customer, their account holdings and their transactional behaviour, in a single location. Loader provides a high performance, resilient and flexible interface - multi-threading, inbuilt error management, reporting and recovery are all standard features. A graphical front end enables users to configure and manage the load scripts
- + **Profiler** offers an array of sophisticated profiling techniques to ensure that all monitoring is targeted and focused, based on past behaviour, predicted behaviour and risk profiles. All customers, accounts and transactions can be risk profiled. The profiles and risk profiles subsequently form the basis of the detection algorithms and provide insight into the customer. Using Breakpoint analysis, Profiler does just this, factoring in multiple risk profiles at multiple levels
- + **Analyser**, the engine at the heart of the SAM solution, performs sophisticated transaction monitoring to highlight

potentially suspicious activities. Analyser delivers high quality exceptions for high-risk behaviour, whilst minimising false positive rates. Analyser uses a number of refined detection techniques to identify and alert behaviour that is likely to represent elevated risk. This covers transaction monitoring, Breakpoint profile analysis and list monitoring.

A series of pre-built, parameter-driven rules are provided as standard. Parameters can be easily tuned to meet the specific requirements of each financial institution. All rules can be risk-weighted and all exceptions risk scored based upon the threat they pose; composited from the customer, account, transactions and rule. All exceptions can be aggregated and rolled-up to the account or to the customer level, to enable a holistic view of the customer's behaviour. A graphical front-end is provided to enable the Compliance Officer to test and manage the detection rules

- + **Investigator** ensures that alerts are raised, routed and managed in a consistent and timely manner. The entire

case management process is workflow-driven, secure and fully audited. All customer, account and transaction data is available instantly to give context to each and every exception.

Investigator provides a sophisticated, intelligent environment to manage the exceptions triggered by the detection scenarios and also those raised by branch or front office staff. All the necessary supporting information upon which to base a decision is instantly available. Customer and account behaviour can be displayed graphically.

“Global spend on AML programs is estimated at US\$3.6 billion in 2006. Personnel costs make up 65% of this”

Celent, 2008

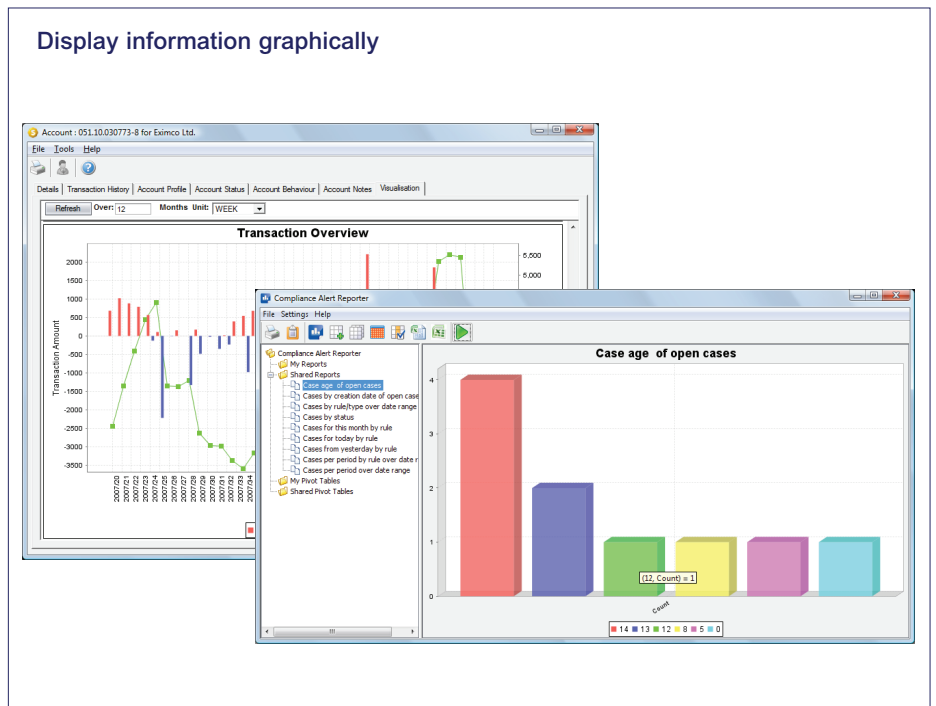
Within Investigator, there are three functions as follows:

- **Case Management** – all relevant information relating to a case is easily captured and recorded, including electronic storage of document images, faxes, correspondence and emails. Cases are tracked, prioritised and managed
- **Workflow** – processes support all facets of the investigation, ensuring compliance with business and regulatory requirements. This workflow includes the facility to refer cases to colleagues with automated notification and generate automated emails
- **List Manager** - allows you to efficiently control, manage and update your watch lists, including internal 'Hot lists', regulatory and third party data. Customer name and address details are monitored against the watch lists and a utility is provided to interactively import lists contents from Excel spreadsheets or CSV files. For banks dealing with high volume payments and bulk watch list filtering, Misys offers a specialist Watch List Checking solution.

+ **Reporter** is the management information module. Reporter provides a series of pre-built reports as well as the ability to create new reports using a point-and-click interface. All information and knowledge contained within the SAM database can be extracted and presented for MIS purposes. Reporter is designed to be simple to use, with a comprehensive range of pre-built management information reports, all of which can be customised. Advanced capabilities are provided for graphing, cross-tab and pivot tables.

Additionally, any report can be scheduled to run automatically and distributed via email to all interested parties, as well as being exported to Microsoft Excel.

Display information graphically



An end-to-end example

Once the overnight batch has been completed on the Misys system(s), transactions from the previous day, together with any updated accounts and customers are extracted and loaded into the SAM database. Newly acquired customers and newly opened accounts are also added to the database.

Every account with transactions for the previous day is re-profiled as the data is loaded. This entire process is automatic and requires no user intervention or input.

The detection rules are run after the account profiling has been completed. The detection rules examine relevant customers, accounts and transactions to see if they trigger any of the initial detection rules. This selection process is automatic and requires no user intervention or input. Any rule breach results in an Exception.

Once all of the automated rules have run, all Exceptions are risk scored, aggregated and converted into Investigation Cases where necessary. These Cases are passed through to the appropriate investigator or team.

Each member of the investigations or AML team will have their own secure login, which determines the cases they receive and the level of authority they have during the investigation.

When the investigator logs in, he/she will be presented with any new or outstanding cases that need attention. From here, these cases can be accessed immediately. When selecting a case to review, investigators are presented with full information on the exception, the transaction, account and customer. They will be automatically guided through the appropriate investigative steps. A full audit is maintained.

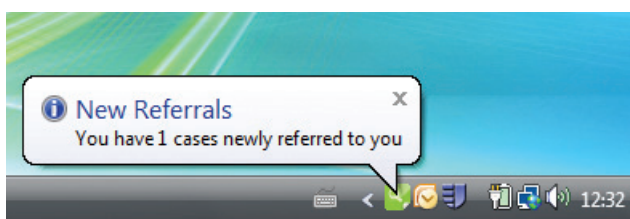
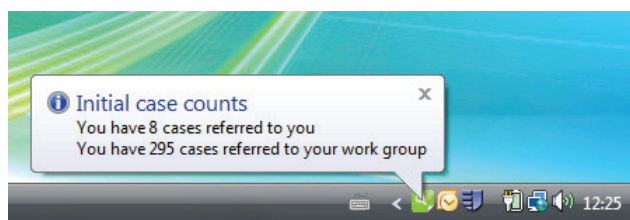
For regulatory investigations, the ultimate aim is to progress each Case through a series of phases to the point of reaching an assisted decision as to whether to submit a SAR (Suspicious Activity Report) or not. At this point, the Case will either be sent for reporting to the FIU (Financial Intelligence Unit) and subsequent followup, or archived. Archived Cases are still available, so that a full picture of account activity is maintained over time.

If it requires non-regulatory action, each step of further investigation will be contained within the system providing a single point of reference for the investigator. In both instances all the information feeds into the Reporter module for operational and risk reporting.

Contact Misys for more information

Transaction monitoring has become the most significant weapon in the armoury of the compliance professional. Misys Suspicious Activity Monitoring enables banks to adopt this risk based approach, thereby focussing effort on key compliance responsibilities and ensuring a consistent, documented approach to preventing financial crime.

Automatic alerts and notifications



To find out how Misys can help you effectively meet your compliance objectives, please contact your Misys account representative.

'Misys' is a trade mark of Misys Plc, a mark registered in various countries worldwide. Midas is a trade mark of Misys International Banking Systems Limited and/or Misys group companies. All other product and company names may be trade marks of their respective owners.

Copyright © 2007 Misys Services Limited. All rights reserved.

Misys Services Limited is a member of the Misys group of companies.
Registered in England, No. 01941076 Registered Office: Burleigh House, Chapel Oak, Salford Priors, Evesham, WR11 8SP