Take control of your correspondent risk monitoring

New Compliance Analytics module supports enhanced AML and CFT compliance for correspondent banking

Benefits

- Supports fact-based KYC reviews and thematic reviews of correspondent activity
- Provides unique, global, top-down view for robust correspondent banking AML/CFT compliance
- Delivers automated notifications to guide and focus AML/CFT investigations
- Supports risk-based approach to correspondent banking compliance
- SWIFT-hosted utility solution is easily imbedded in BAU operations

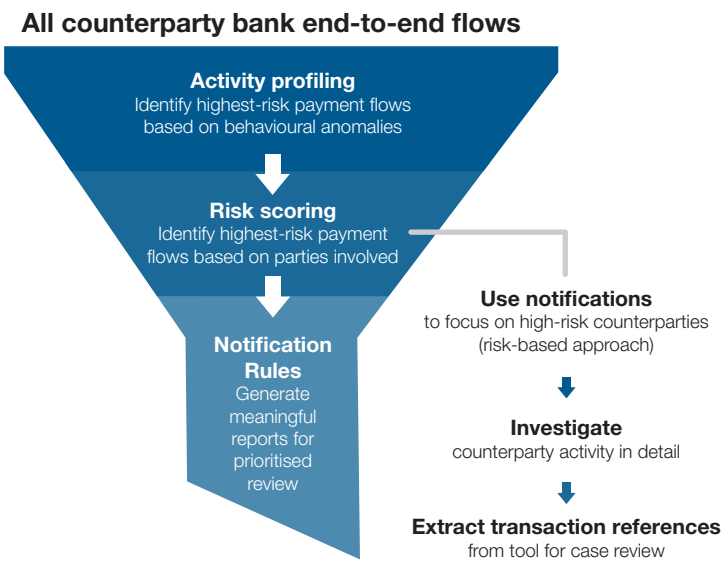
Features

- Activity profiling – 75 risk metrics for correspondent relationships and transaction activity
- User-driven parameters and rules for anomaly detection
- Risk scoring and modelling to identify highest-risk areas
- Single, standardised overview across your global organisation based on group-wide data
- Cloud-based service with no hardware or software to install or maintain

International regulatory and oversight bodies, including the Financial Action Task Force (FATF), the Basel Committee on Banking Supervision (BCBS) and The Wolfsberg Group have highlighted the need to strengthen ongoing due diligence and AML monitoring of correspondent banking relationships.

All correspondent banks are expected to establish appropriate AML/CFT policies and controls in order to detect any activity that is inconsistent with the objective of services provided to the respondent bank, or that is contrary to the existing commitments between the correspondent and the respondent. Institutions are encouraged to strengthen their AML/CFT tools in order to evaluate specific risks for each of their correspondent banking relationships.

SWIFT has developed Correspondent Monitoring in close collaboration with customers to provide a tool that addresses the specific requirements and challenges of correspondent banking AML/CFT compliance.



Correspondent Monitoring's global, top-down approach is designed specifically to support correspondent banking AML/CFT compliance.

Focus on correspondent banking

Correspondent Monitoring is a module within Compliance Analytics that has been designed specifically for monitoring correspondent banking relationships at group level. It generates reports that can be used on an ad-hoc basis to support periodic KYC reviews, as well as thematic reviews of correspondent activity such as country or currency exposure.

The reports can also underpin business as usual AML/CFT compliance activity. They enable banks to automatically monitor SWIFT payment traffic to detect unusual patterns that merit further manual review as part of BAU compliance processes.

How does Correspondent Monitoring work?

Unlike most AML solutions, Correspondent Monitoring takes a top-down approach that combines activity profiling, notification rules and risk scoring to generate detailed reporting for user review. The reporting facilitates a risk-based approach to correspondent monitoring by highlighting higher-risk payment flows for additional monitoring and investigation in line with institutional policies.

Activity profiling

Activity profiling leverages over 75 metrics to evaluate correspondent relationships based on transaction activity. These combine general metrics (e.g. values, volumes, and behavioural comparison with past activity) with nesting (type, number of nested relationships, scale of services) and beneficiary metrics. The activity metrics detect the extent to which specific activity differs from expected norms.

Rules and notifications

Notification rules are created using combinations of activity metrics. Each rule specifies a pattern that should generate a notification for user review when it occurs. The tool provides default rule templates that users can edit in line with (evolving) institutional policy and risk appetite. The risk score is optionally used within notification rules and reporting to facilitate a risk-based approach to correspondent banking AML/CFT compliance.

Risk scoring

Each correspondent banking payment chain involves a combination of originating, beneficiary, and counterparty banks. Correspondent Monitoring assigns each flow a risk score based on aggregated risk factors associated with the banks involved in the chain and the relationships between them, independent of transaction value or volume.

Risk factors are defined by the Correspondent Monitoring customer and can include the risks of countries and banks, the role of the banks (originator, beneficiary, intermediary), and the type of nesting taking place.

User settings and reporting

Correspondent Monitoring lets users apply rules at three levels of granularity, matching the three levels of granularity in the reporting. These levels are:

- **Counterparty level:** statistics relating to a specific counterparty or respondent.
- **Nested relationships level:** statistics for interactions between a specific counterparty and nested originator(s) or beneficiary(s).
- **Message Flow Level:** statistics on interactions between specific combinations of banks in a payment chain, from originator to beneficiary.

Easy to set up and use

As a Correspondent Monitoring subscriber, you benefit from SWIFT's compliance utilities approach: secure, SWIFT-hosted solutions that are easy to implement, have no hardware or software to install or maintain, and have been developed in collaboration with our community.

Correspondent Monitoring leverages your global SWIFT traffic data, eliminating the need for time-consuming data collection and transformation and costly IT projects. SWIFT experts will train you to use the tool and set up customised reporting and notifications as part of your business as usual AML/CFT correspondent risk monitoring programmes.

Compliance Analytics

Correspondent Monitoring complements SWIFT's broader Compliance Analytics and AML services offering. It leverages SWIFT message data to provide unparalleled insight into your institution's global banking flows, enabling you to monitor and address financial crime risk with pinpoint precision.

Built around a secure, state-of-the-art and user-friendly data mining platform, Compliance Analytics uses advanced data visualization to aid analysis and generates notifications when detecting spikes, outliers or policy breaches.

It helps you compare your message traffic with global aggregated traffic over SWIFT, highlighting, for example, your share of payments traffic in a particularly high-risk country.

A separate data analytics service, Payments Data Quality, enables banks to determine the quality of originator and beneficiary information in the payments messages they send and receive.

In addition to supporting compliance with FATF Recommendation 16 and related regulation about originator and beneficiary information in payments messages, Payments Data Quality helps banks increase straight-through processing and enhance payments efficiency and transparency.

More information
SWIFT offers a growing portfolio of financial crime compliance services that address customer needs in the areas of sanctions, Know Your Customer (KYC), AML and fraud prevention. Learn more at www.swift.com/complianceservices

For more information, contact your SWIFT account manager or email Compliance.Analytics@swift.com

57224 - March 2017