Information Paper

How big is your KYC data?

Access to high quality, standardised data is key to keeping on top of your KYC requirements

Contents

As regulators around the world raise the bar on banks' Know Your Customer (KYC) requirements, access to a set of industry-wide, high quality, standardised data is paramount to help banks align their KYC compliance programmes. Expectations are high – so how can SWIFT help you manage these requirements more effectively?

The growing KYC burden

As financial institutions' onboarding teams spend more time collecting data from different sources, Due Diligence managers face considerable challenges. It's essential to be able to collect accurate and up-to-date data and documentation relating to new clients and counterparties, as well as reviewing existing counterparties. However, the tasks involved are often manual and time consuming, and understanding the requirements across different jurisdictions is less than straightforward.

Consequently, the prospect of being able to access standardised data in a single location is compelling. The more easily the necessary information can be accessed, the more time Due Diligence managers can spend carrying out analysis and making sure that business relationships are up and running.

Increasing expectations

Regulators expect banks to know their customers better than ever before. Basic details about a client's identity are not enough. You need to understand who your correspondents are, who owns them, in which jurisdictions they operate, what products or services they offer and to whom. You also need to understand and monitor their behaviour on an ongoing basis.

Ultimate beneficial ownership (UBO) has also recently come under the spotlight. Typically banks are required to verify the identity of any UBO that owns 25% or more of a company opening an account. However, in Europe the Fourth EU Anti-Money Laundering Directive (AMLD4) has recently reduced this threshold to 10%. Regulators also increasingly require banks to understand and account for the full ownership hierarchy, rather than just direct UBOs.

What are the challenges?

Stricter regulatory requirements are forcing banks to adjust their policies and procedures and move towards a risk-based approach. This means that as a due diligence manager you need to collect more information than ever before in order to carry out enhanced risk assessments. Based on your assessments, you can then make informed decisions on whether to start a relationship with a new bank or counterparty, or continue an existing one.

Clearly, this calls for more resources to cope with the increased workload, which includes one off and recurring activities such as data collection, validation, analysis and risk assessments. These can be both costly and time consuming, especially if the information is procured bilaterally. But it pays to get it right, or you run the risk of being in breach of regulations.

How much information?

Not all KYC is equal. With banks increasingly expected to adopt a risk-based approach, the way in which KYC requirements are managed varies considerably across different institutions and jurisdictions. As a result, not only are banks asking for more information overall – different banks are also asking for different sets of information.

Wolfsberg guidelines

- For **Foreign Correspondent Banking relationships**: banks must carry out adequate risk-based due diligence when payment-related information is (or will be) exchanged with a counterparty. For the exchange of non-payment-related information, this may be unnecessary. However, the appropriate level of due diligence will be needed if the correspondent has an account or a client relationship with the institution.
- For banks that have exchanged **Relationship Management Applications (RMAs) on the SWIFT network**, the level of due diligence required varies according to the nature of the counterparty relationship. RMA requests can be segregated between customer and non-customer RMAs, with distinct due diligence criteria for each.

Containing the costs

Regulators do not explicitly state what information is required to comply with due diligence requirements, so banks tend to ask counterparties for an extensive list of KYC documents and data. This list is tailored to the requesting institution's risk appetite, policies and procedures. Banks are expected to act in good faith based on the information that is provided – and consequently some have opted to terminate relationships in order to contain the associated efforts, costs and risks.

The KYC Registry: understanding your needs

With so many aspects of KYC compliance open to inconsistencies, a set of industry-wide KYC data and documentation is essential to help banks align their KYC compliance programmes. This way, banks can share information centrally, rather than repeatedly asking each other for the same KYC information – and they can achieve substantial efficiency gains as a result.

Built by SWIFT, The KYC Registry is a shared utility platform that allows banks to upload and share a standardised set of KYC data and documentation. This was developed in collaboration with the world's largest correspondent banks to address large banks' KYC requirements across different jurisdictions, and provide smaller institutions with a global standard for KYC compliance.

How standardisation can help

Information in The KYC Registry is divided into five broad categories:

1. Customer identification (regulatory statutes, contact details, regulator, proof of existence)
2. Ownership and management structure (key controllers, ownership, shareholders, UBOs)
3. Type of business and client base (type of products and services, customer base, geographical presence and operations, business with sanctioned countries)
4. Compliance information (policies and procedures, compliance contact information)
5. Tax information (TIN, FATCA information including GIIN, CRS information)

You can use the Registry to share your own KYC data with your correspondents, obtain KYC data from your counterparties, or both. Counterparties can also communicate with each other via the platform. Data contributors submit the required documents and information, which SWIFT checks and validates. Approved users can then access the information they need in order to facilitate client onboarding, support periodic reviews and manage trigger events, in a standardised format.

The KYC Registry helps you to carry out detailed due diligence checks when onboarding new counterparties, reducing the time it takes to start doing business. It also supports ongoing due diligence by flagging up important changes at counterparty institutions.

Recipe for success

Critical mass is required for a large community of banks to benefit from real efficiency gains. With over 4,500 banks joining The KYC Registry in the first three years, the utility has rapidly gained traction – and the number of members continues to grow. KYC Registry member banks represent 75% of total SWIFT message traffic, and new banks are joining all the time.

Data privacy is essential as the information shared includes personal information about UBOs and key controllers. KYC as such is not a new process; banks have long been required to share this type of information using different channels, including physical transmission by fax and telephone. By using the Registry you can decide which of your counterparties is granted or denied access to your data and is comfortable sharing information using this permission-based method.

Quality of information is also vital. Correspondent banks are required by regulators to ensure that the information they collect is 100% accurate, so outsourcing this responsibility to a third party is not an option. You can rely on the accuracy and validity of the data on The KYC Registry, since it:

- is uploaded by the banks themselves
- is validated by SWIFT
- contains a date stamp indicating that the information is up to date

You and your customers can now enjoy the resulting efficiency gains, cost savings and business opportunities.

Not all data is equal

The quality of KYC data varies. Banks generally deal with static data, such as names, addresses and details of ownership, which can usually be validated. But in the context of KYC, 'data' is mostly self-declared behaviour. This includes information on a range of topics, including the bank's products, services, geographical footprint and AML training programme.

While self-declared information cannot be validated in the same way as static data, the information added to the Registry is a bank's public statement about its approach to different compliance topics, similar to information posted on its website. This information is made available to all relevant counterparties, providing a single, consistent answer to each question. KYC information is also distributed consistently to all counterparties, removing the risk that a bank is selective or inconsistent in its answers.

Validating KYC information

Any static data uploaded to The KYC Registry has to be validated by SWIFT's compliance experts before it can be shared with counterparties. The validation process involves reviewing and cross checking all data and documents against three key criteria:

1. **Completeness:** Has the bank provided all the information required? Is anything further needed?
2. **Validity:** Is the information valid and up to date?
3. **Accuracy:** Is the information correct? Are there any discrepancies between the different documents and data points?

The KYC Registry: data benefits

- **Data security:** Banks can choose which of their counterparties can access their information.
- **Validation by SWIFT:** Provides reassurance about the accuracy of data published on The KYC Registry.
- **Consistent answers:** Banks publishing their data on the Registry provide a single, consistent answer to each question.
- **Up-to-date information:** Data is date stamped and regularly updated, with options for counterparties to request updates or clarifications.
- **Alerts for updates:** Banks accessing their counterparties' information are alerted when any changes are made.
- **Enhanced data option:** Banks will have the option of sharing a more confidential set of data later this year.

Keeping up to date

KYC information can and does change over time. Some regulations stipulate that certain data is valid for only three to six months. If you are carrying out a KYC check on a respondent, you need to be sure the relevant information is current. You may therefore need to ask your counterparties to confirm or certify data from time to time, which increases workload.

Members of The KYC Registry are obliged to keep all their data current and update the relevant details promptly when any changes occur, such as updates to the organisation's key controllers or the beneficial ownership structure. Any such changes will trigger the validation cycle, with notifications automatically sent to the bank's counterparties alerting them to the changes.

Banks demonstrate a diligent approach to keeping their information current and making changes when needed. SWIFT also prompts banks to update their data if this has not been done recently. You can communicate directly with your counterparties via the Registry if there is any requirement for clarification, and can request updates or confirmations that the data displayed is still valid. You can also ask your counterparties for additional information specific to your local KYC requirements.

Forging ahead

The KYC Registry continues to evolve apace, with a number of milestones reached this year.

- As regulatory requirements evolve, the Registry's baseline – in other words, the standard set of KYC data and documents held on the Registry – has been increased from 150 items to around 500 to meet the most stringent regulatory requirements. The new baseline differentiates between basic and extended KYC information, allowing banks to decide which level of information they wish to share.

- As part of this evolution, SWIFT has aligned The KYC Registry baseline with the new Wolfsberg Due Diligence Questionnaire (DDQ) for Correspondent Banks. This ensures coverage of up to 90 percent of the information correspondent banks typically require for KYC compliance, delivering major time and cost savings.

- SWIFT's KYC Adverse Media service provides curated content and regulatory notifications related to any member of The KYC Registry. Users can also access information about banks that have not yet joined the Registry. This helps you to factor in negative news coverage as part of a risk-based approach to compliance.

The quest for efficiency

With increasing pressure on banks to provide more comprehensive KYC information to meet myriad regulatory obligations, the financial industry as a whole is seeking opportunities for more efficient ways of working. This is certainly the case for Due Diligence managers, who have much to gain by accessing information in a standardised and streamlined way.

The KYC Registry allows banks to share and procure accurate and up-to-date KYC data in a standardised and centralised way. And with this comes the potential for efficiency gains, greater transparency and cost control, both for individual banks and at an industry level. For Due Diligence managers, this can provide an opportunity to streamline processes, gather information more efficiently – and get business relationships up and running at the earliest opportunity.

For more information visit
www.swift.com/complianceservices
or contact your account manager

About SWIFT

SWIFT is a global member-owned cooperative and the world's leading provider of secure financial messaging services.

We provide our community with a platform for messaging, standards for communicating and we offer products and services to facilitate access and integration; identification, analysis and financial crime compliance.

Our messaging platform, products and services connect more than 11,000 banking and securities organisations, market infrastructures and corporate customers in more than 200 countries and territories, enabling them to communicate securely and exchange standardised financial messages in a reliable way. As their trusted provider, we facilitate global and local financial flows, support trade and commerce all around the world; we relentlessly pursue operational excellence and continually seek ways to lower costs, reduce risks and eliminate operational inefficiencies.

Headquartered in Belgium, SWIFT's international governance and oversight reinforces the neutral, global character of its cooperative structure. SWIFT's global office network ensures an active presence in all the major financial centres.

For more information,
visit www.swift.com
or follow us on
Twitter: @swiftcommunity
and LinkedIn: SWIFT.

Trademarks

57340 - December 2017