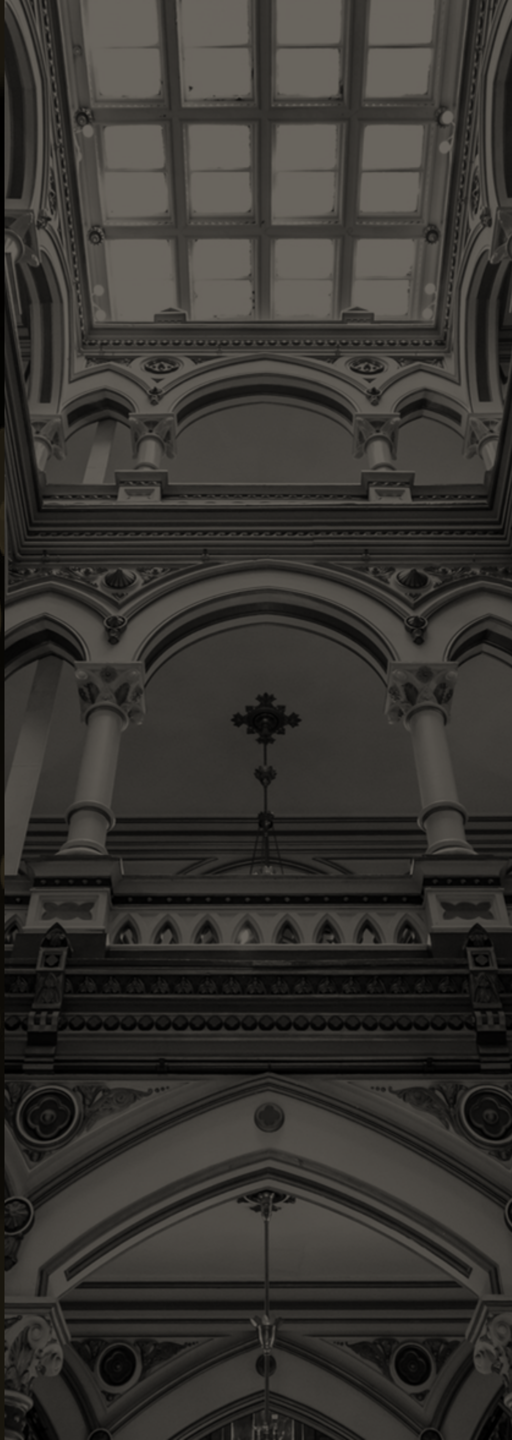
SPOTLIGHT ON KYC PROCEDURES

Knowing Your Customer Data Journey

A Spotlight on Standards for Know Your Customer (KYC) Framework and Procedures



StratisAdvisory

RISK | STRATEGY | CYBER COMPLIANCE MANAGEMENT

The KYC Framework

Know Your Customer (KYC) is a significant element in today's fight against financial crime and money laundering. KYC is a regulatory obligation for almost any institution that interacts with money. Standard KYC procedures generally apply when a business onboards a new client or a current client acquires a regulated product. KYC is an ongoing process, consisting of multiple steps throughout a customer's lifecycle.

Customer Identification Program (CIP)

Collection of customer information, a minimum standard of information which is sufficient to, upon verification, establish the true identity of each customer.

Risk-Based Approach Verification

- Documentary Verification
- Non-Documentary Verification

Information Collection

Legal Entity

- Entity Name and Type
- Corporate Identification Number
- Physical Address
- Contact Information
- Formation Documents

Individual

- Name
- Physical Address
- Date of Birth
- Individual Identification Number
- Government-Issued Photo Identity Document

Customer Due Diligence (CDD)

Obtaining and analyzing sufficient customer information to understand the nature and purpose of each customer relationship, including understanding the types of transactions a customer will likely engage in.

Enhanced Due Diligence (EDD)

Collecting additional information, performing additional verification, or more frequent/detailed review when CDD determines a customer poses a higher risk of financial crime.

BANK OBLIGATIONS AND DATA

- Bank's must gather both proof of identity ("POI") and proof of address ("POA") for each customer, at minimum, prior to establishing an account.
- The minimum requirements for customer identification include the following: Full Name, Date of Birth, Address, Identification Number and Tax Number.
- It is important to note that the same document cannot be used to confirm both the customer's identity and their place of residence. Thus, at least two (2) documents are required for the KYC process.
- For each customer for which a bank maintains an account, this information must be collected and verified.

NON-BANK RESPONSIBILITIES

- Non-bank customer identification requirements are primarily risk-based. Unlike a bank, they generally do not have specific regulations for collecting information.
- Typically, non-banks collect and retain the following: Full Name, Date of Birth, Address, and Identification Number.
- Transfers over a certain threshold, made in person or online, may require additional controls such as verifying the identity of the person by obtaining and retaining a record of an identification document. Rather than the copy or record of the method of payment.
- Non-banks may not have the same regulations as their banking partners. However, enforcement and compliance of the regulatory requirements are inherent in upstream partnerships.

UNLOCKING THE POTENTIAL OF KYC DATA

- The submission of KYC documents and the process of checking them is partial to an AML framework. The goal of AML is to verify with a high degree of assurance that customers are whom they say they are and that they are not likely to be engaged in criminal activity.
- The verification process enables companies to capture customer demographic data, which can be integrated into enterprise systems such as email address, IP, Geolocation, device fingerprint, session log in info, transacting location.
- The data collected through the KYC process enables companies to streamline the customer onboarding process, conduct further due diligence, risk assessment and optimize politically exposed persons (PEP), sanctions, and watch lists investigations.
- An enhanced KYC journey enriches customer risk profiles, and better aligns resources and technology for risk mitigation. The less information a company collects, the less information the company gains to analyze the data for business purposes.

Discover what Stratis Advisory can do for you

Customer Journey Development

Developing a customer journey is dependent on your user experience design, but also contractual requirements with partners, regulatory requirements, and best practices to mitigate risk. Stratis can help you design your customer journey to align with your user experience, recommend where to add risk mitigants, identify the appropriateness of vendor solutions, and satisfy KYC, privacy, and business model relevant disclosures.

Customer Experience Data Analysis

From the earliest interactions with a user to collecting Personally Identifiable Information (PII), customer interactions leave behind a data trail that can be leveraged for marketing, security, and enhanced customer experiences. Stratis can help you evaluate existing onboarding and due diligence processes to ensure your data gathering meets regulatory requirements, appropriate disclosures, and data retention requirements as a data controller or processor.

Data Privacy Risk Assessment

From collecting basic platform usable information on a user to collecting customer information such as personally identifiable information (PII), how you collect, gather, store, transfer, and use such data is critical to maintaining compliance with various global privacy laws. Stratis can assess your current and future data gathering practices as you open new markets, acquire companies, and launch new products that require different customer disclosures.

StratisAdvisory

LAUNCH | SCALE | OPTIMIZE

Stratis Advisory | 1.415.352.1060 | www.stratisadvisory.com | info@stratisadvisory.com