# Building Intelligence into Financial Crime Compliance

Organizations are under pressure to improve their financial crime compliance, while at the same time trying to reduce operational costs and improve customer experience. Balancing these demands requires a reconsideration of operating models for anti-money laundering (AML) and know your customer (KYC) compliance, and the re-engineering of supporting IT infrastructure and applications.

| AML Components | KYC/CDD | Screening | Transaction Monitoring | Case Management |
|---|---|---|---|---|
| **Data Challenges** | • Subjective segmentation<br>• Lack of data for risk sensitive customer profiling<br>• No single Customer view | • Challenge in managing changes across multitide of lists<br>• Name, Other data quality issues | • Population groups for setting thresholds is not risk based<br>• Incomplete mapping product codes to Transaction codes, coverage | • Difficult to correlate data across components<br>• Lack entity resolution |
| **Technology Challenges** | • Limited capability for behaviour analysis, link analysis | • Extracting information from documents | • Lacks capability to process large data sets and identity patterns | • Highly Manual task<br>• Lacks Visualisation capability |

Figure 1: Breakdown of AML challenges and how they manifest across financial compliance infrastructure.

An intelligent, driven approach requires organizations to improve their use of data and advanced analytics. This can be supported by artificial intelligence and machine learning. The aim is to reduce false positives and detect suspicious activity early, while managing the cost of operations.

Volume, velocity, veracity and variety of data transactions is driving banks to redesign their data, process, application and technology architectures.

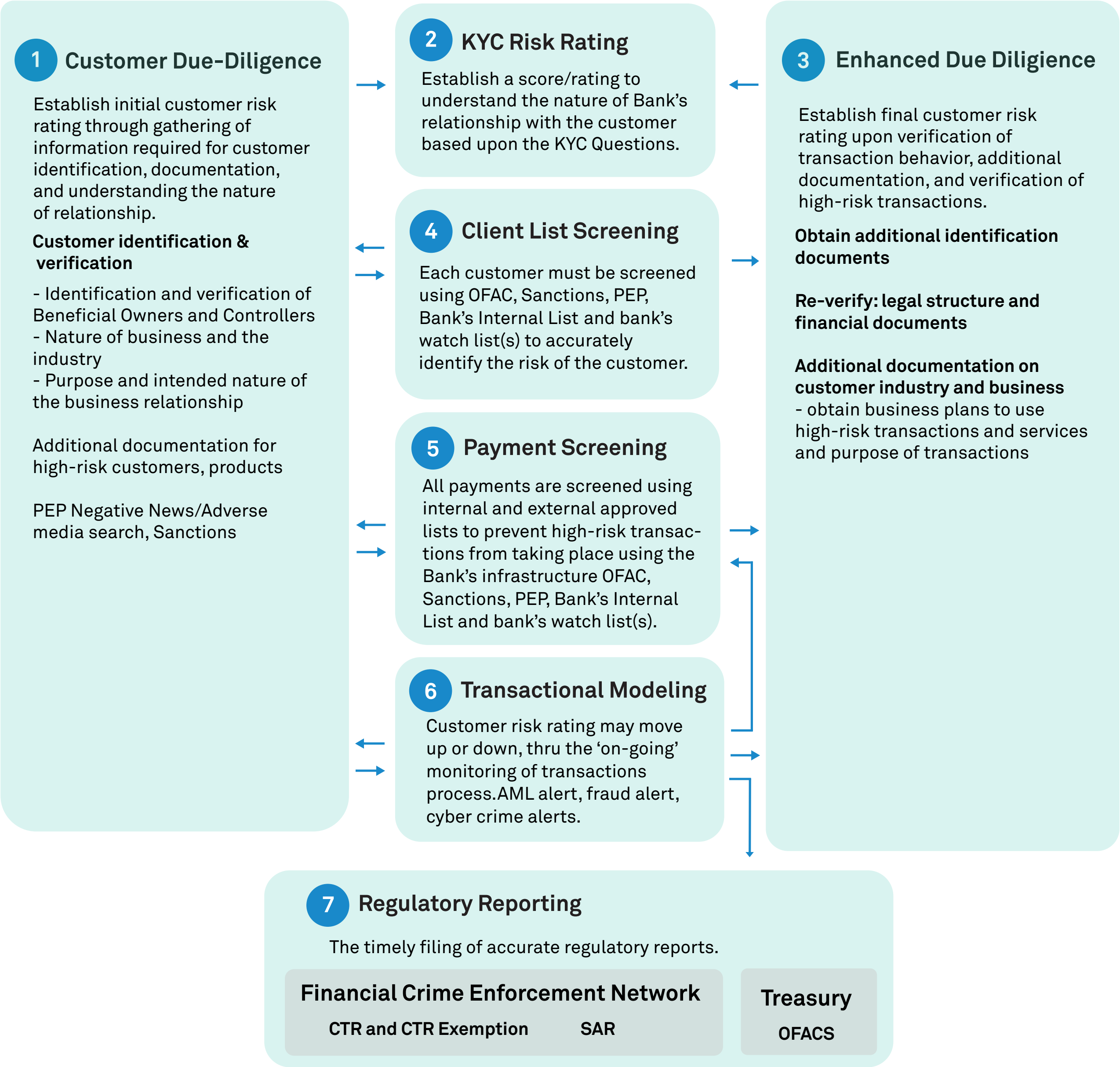
The amount of data required to meet financial crime compliance is increasing at an exponential pace. Current data and analytical infrastructure is unable to cope with this increase.

The accuracy of the data also needs to improve significantly. Data needs to be current at all times. Firms are moving away from periodic reviews of KYC data, and are instead using changes in material data to trigger reviews.

It is also important to dissolve organizational silos. This allows for the sharing of data, customer behavior and intelligence, to further increase the quality of the data and its ability to help detect money laundering and fraud. In the past banks set up operational and technological silos along business units or product processors, resulting in higher costs for financial crimes compliance. Existing technology infrastructure has limited capacity and is unable to support the risk-based approach recommended by regulators.

To combat this, banks are implementing, augmenting and automating customer data collection mechanisms, in the front office and from relationship managers. IT architectures that support AML/KYC are being redesigned to resolve data fragmentation across silos, and common data models are being built, supported by semantic layers. The IT architecture needs to be engineered to support a minimum growth of 25% in processing and storage capacity every year until effective data archival and purging plans are implemented.

Figure 2 illustrates a target architecture to support financial crime compliance. This is an integrated architecture, that sits across all silos and financial crime types—KYC, money laundering, fraud and cyber:



**1 Customer Due-Diligence**

Establish initial customer risk rating through gathering of information required for customer identification, documentation, and understanding the nature of relationship.

**Customer identification & verification**

- Identification and verification of Beneficial Owners and Controllers
- Nature of business and the industry
- Purpose and intended nature of the business relationship

Additional documentation for high-risk customers, products

PEP Negative News/Adverse media search, Sanctions

**2 KYC Risk Rating**

Establish a score/rating to understand the nature of Bank's relationship with the customer based upon the KYC Questions.

**3 Enhanced Due Diligence**

Establish final customer risk rating upon verification of transaction behavior, additional documentation, and verification of high-risk transactions.

**Obtain additional identification documents**

**Re-verify: legal structure and financial documents**

**Additional documentation on customer industry and business**
- obtain business plans to use high-risk transactions and services and purpose of transactions

**4 Client List Screening**

Each customer must be screened using OFAC, Sanctions, PEP, Bank's Internal List and bank's watch list(s) to accurately identify the risk of the customer.

**5 Payment Screening**

All payments are screened using internal and external approved lists to prevent high-risk transactions from taking place using the Bank's infrastructure OFAC, Sanctions, PEP, Bank's Internal List and bank's watch list(s).

**6 Transactional Modeling**

Customer risk rating may move up or down, thru the 'on-going' monitoring of transactions process.AML alert, fraud alert, cyber crime alerts.

**7 Regulatory Reporting**

The timely filing of accurate regulatory reports.

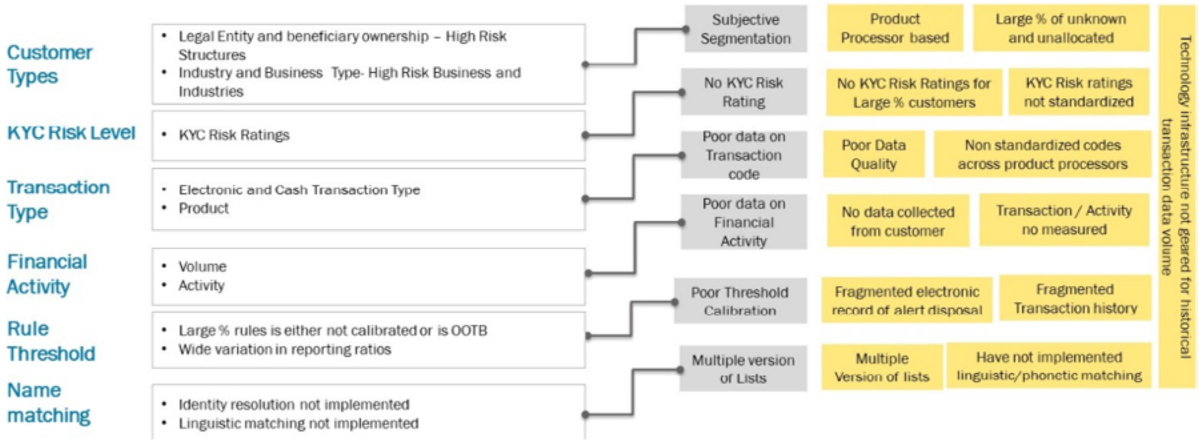
**Financial Crime Enforcement Network**

**CTR and CTR Exemption** **SAR**

**Treasury**

**OFACS**

Figure 2: Model of an integrated architecture supporting financial crime compliance for KYC, AML, fraud and cyber.



| | | | | |
|---|---|---|---|---|
| Customer Types | • Legal Entity and beneficiary ownership – High Risk Structures<br>• Industry and Business Type- High Risk Business and Industries | Subjective Segmentation | Product Processor based | Large % of unknown and unallocated |
| KYC Risk Level | • KYC Risk Ratings | No KYC Risk Rating | No KYC Risk Ratings for Large % customers | KYC Risk ratings not standardized |
| Transaction Type | • Electronic and Cash Transaction Type<br>• Product | Poor data on Transaction code | Poor Data Quality | Non standardized codes across product processors |
| Financial Activity | • Volume<br>• Activity | Poor data on Financial Activity | No data collected from customer | Transaction / Activity no measured |
| Rule Threshold | • Large % rules is either not calibrated or is OOTB<br>• Wide variation in reporting ratios | Poor Threshold Calibration | Fragmented electronic record of alert disposal | Fragmented Transaction history |
| Name matching | • Identity resolution not implemented<br>• Linguistic matching not implemented | Multiple version of Lists | Multiple Version of lists | Have not implemented linguistic/phonetic matching |

Technology infrastructure not geared for historical transaction data volume

Figure 3: Six key challenge areas faced by financial firms, and the effects of these challenges on monitoring/screening efforts.

Firms are facing challenges across six key areas, leading to high volumes of false positives in transaction monitoring and list screening (Figure 3). Banks have not been able to refine transaction monitoring. As a result, list screening is the predominate method. To compensate, banks have implemented lower thresholds, generating higher volumes of false positives.

To address these collective challenges, banks are transforming their AML and KYC target operating models, focusing on four key areas:

- **Standardizing and consolidating rules and technologies across business areas**
  This includes the creation of global financial crime policies with standardized procedures for KYC, AML and sanctions screening across the globe, that meet the range of regulatory requirements. Firms are also standardizing approaches across channels, eliminating redundant technology platforms and resources. They are leveraging data and other core functions, utilizing robotic processing and hyper-automation to build service models that prevent financial crimes.
- **Implementing risk-based approaches (RBAs)**
  RBAs use KYC risk ratings to identify high-risk customers and transactions. A risk-based approach must include granular-level customer segmentation, which may use machine learning or other analytical methods such as topological data analysis to establish segments and thresholds, and screen for false positives.
- **Refreshing transaction monitoring and screening systems on big data platforms**
  The increasing volume of data and the move to risk-based approaches requires firms to revise their transaction monitoring and screening systems for big data platforms. For the best return on this investment, firms should communicate with fraud and cyber to allow a comprehensive view of financial crime data and results. A single platform allows firms to run multiple analytical solutions for financial crimes, providing greater flexibility and access to the proper methodology for any particular problem. Re-implementation of platforms also standardizes customer and product scenarios, reducing redundancies across AML and fraud.
- **Implementing enterprise-wide case management tools.**
  Case management tools offer a range of benefits:
  - Drive efficiencies in alert management
  - Support case investigation, analysis, compliance; check truncation systems, and reporting for suspicious activity and fraud
  - Provide entity/identity resolution, natural language processing and understanding, statistical and machine learning models; configurable workflow capabilities to allow intelligent, contextual and forensic research

  Links between AML, fraud and cyber are increasing. Case management tools need the ability to conduct network link analysis and event correlations.

  Case management tools also modernize platform performance by providing automatic access to, and accumulation of required data from internal and external sources, and digitizing paper-based documents to support the analysis of the alerts.

## In summary

To reduce false positives, and more effectively detect suspicious activity while managing costs, firms must revise their target operating models and infrastructure for financial crime compliance, and build intelligence-driven financial crime capabilities.

**Wipro Limited**
Doddakannelli, Sarjapur Road,
Bangalore-560 035,India
Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

**Wipro Limited** (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 175,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information,please write to us at
info@wipro.com