WHITE PAPER

Enabling Robust Compliance Systems to Combat Financial Crime

– Focus on efficiency and optimization

Infosys®

Overview

While financial institutions (FIs) continue to evolve in the era of digitization, preventing financial crime and managing compliance are equally important to sustain market share and reputation. Financial crime relates to activities against FIs or their customers and comprises money laundering, fraud, market abuse, terrorist financing, bribery and corruption, cyber-crime, and tax violations. As criminals find new ways to break the law, regulatory expectations continue to increase and have widespread implications on FIs. In today's era, where digital payments see an upsurge in volumes and customers adopt new ways to transact, the ability to detect and prevent financial crime becomes critical. On a global scale, FIs incur annual losses of about US$400 billion, due to cyber crimes. Similarly, yearly card fraud losses are estimated to exceed US$35 billion by 2020. It is, therefore, inevitable that FIs continue to invest in customer due diligence and anti-money laundering systems (AML). As per a recent Tower Group research report, 59 percent of banks expect to increase AML systems, this year. Additionally, 38 percent of banks are planning to replace AML systems. Customer due diligence or know your customer (KYC) processes require huge operational costs and must be re-looked at. Currently, FIs use different solutions to manage financial crime and run diverse compliance programs. Managing these compliance programs is difficult, costly, and time-consuming. FIs are now realizing the need for an enterprise-wide strategy, instead of creating solutions in silos.

Key challenges

Some of the key challenges faced by compliance programs are:

Inadequate compliance data management

As per industry analysis, risk and compliance data management is the top area of spend across IT initiatives in this domain, and accounts for over a third of the spend. Challenges of mutiple data sources and complex integration create issues such as inaccurate risk profiling and detection results. Many a time, businesses have discovered data issues post implementation of systems or during regulatory audits and have spent a tremendous amount of effort and money in the rework and remediation process.

Disjointed financial crime view

FIs have invested heavily, over the last several years, in creating multiple systems across customer due diligence, AML, screening, and enterprise fraud. NICE Actimize survey has discovered that 53 percent of large FIs (with asset size of at least US$60 billion) have more than 10 analytic or detection systems and 31 percent have more than 20 systems. However, FIs lack a unified view of customer's profile or suspicious activity across a relationship life cycle, which creates efficiency issues in preventing financial crime.

Cost of compliance operations

Compliance operations continue to be very expensive. Regulatory-driven manual processes and inadequate system automation have possibly not allowed compliance teams to explore opportunities for cost optimization. Based on an industry research, 85 percent of a compliance analyst's time goes in manual data collection during case management activity. Any opportunity of automation without risking the regulatory ask is going to benefit FIs.

Solution recommendations

Compliance management systems are undergoing radical changes such as technology upgrades, expansions of functional capabilities, and complex data integration changes. Data management is a very critical element, which if managed correctly, can bring in efficiencies throughout the life cycle of projects. Investment in business process automation is getting increasing importance, as compliance operations require huge effort and high cost in the overall life cycle. Similarly, application of machine learning is gaining traction to enable systems to learn from data, get insights, and enhance functionality and accuracy.

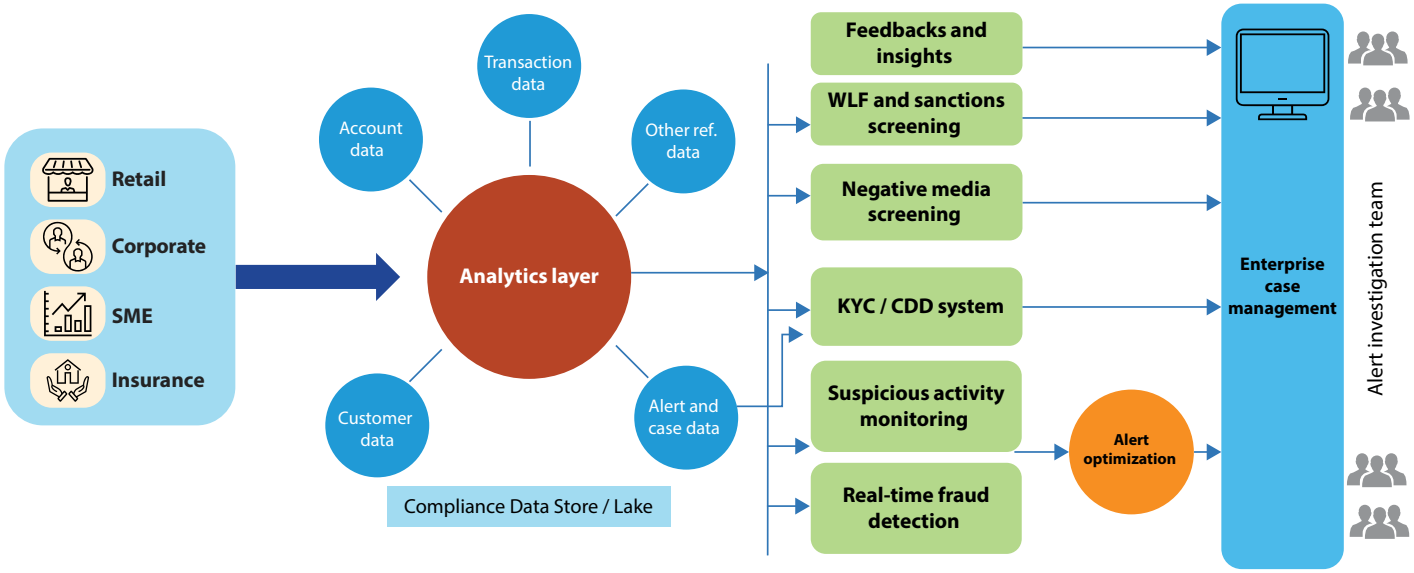


Exhibit 1: Recommended Solution Components

Listed below are a few suggested solutions and considerations to effectively define a robust compliance implementation strategy to detect and prevent financial crime

1. Creating a specific data strategy for financial compliance

Data strategy is key to the success of any anti-financial crime system implementation. Key building blocks of data strategy include:

- **Strategy for data quality assessment**

  High-quality data can enable FIs to implement anti-financial crime management solutions with a much greater accuracy and can help in reducing the effort of ongoing compliance requirements. It is imperative to keep data quality as one of the high-focus tasks, while building the compliance system implementation plan. Strategy for data quality should include:

  - **Data discovery and profiling** – Data discovery and profiling is the process of analyzing data sources to provide information and statistics about the data. It helps to understand source data required and its quality for further mapping and feeding into compliance systems.
  - **Data mapping and transformation analysis** – It is important to map the right set of fields from source systems to target compliance data store and further to compliance systems, from a functional and technical perspective. It is also important to understand critical or mandatory data requirements, missing or incomplete data and its impact on transaction monitoring systems. Analyzing transformation logic used for data transformation requirement is another focus area in data strategy. Validation of currency conversion logic and inclusion / exclusion logic of transaction codes are some examples where transformation analysis and validation is needed for compliance data transformation.
  - **Fixing inaccurate data or inconsistent data** – Accuracy and consistency of data over a period of time is extremely important and a proper strategy is required to fix any inaccuracy either at the source level or at staging layer before feeding into compliance systems.

- **Specific data store for compliance requirements**

  FIs typically route multiple data sources and data stores into compliance systems. This mandates the need to create a consolidated data store or data lake, which can form a staging layer between core data sources and compliance systems.

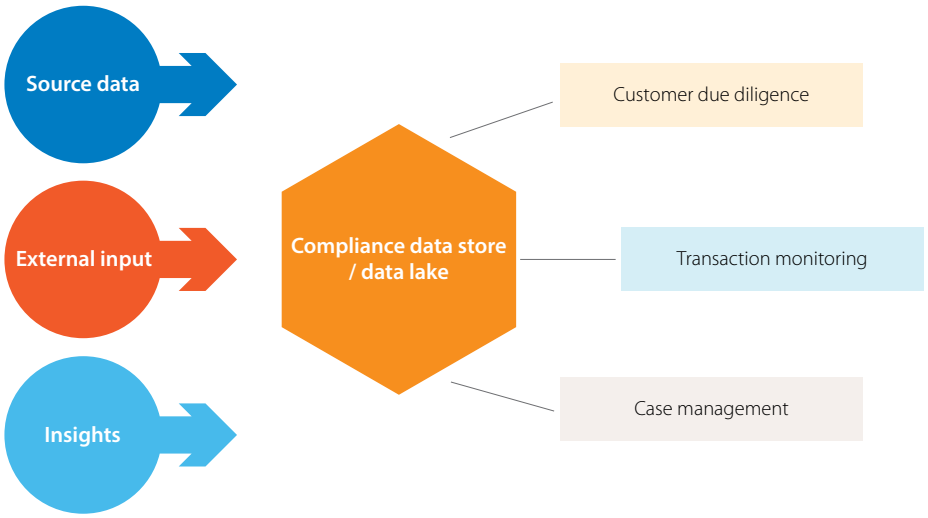


Exhibit 2: Data Strategy for Compliance

This approach reduces the dependency on source systems and enables easier integration. By creating a separate data store, dedicated to compliance data requirements, organizations can ensure easy data discovery and analysis. Compliance data store can also be leveraged by financial crime intelligence units (FCIUs) for the analysis of financial crime scenario logic, functional tuning, analytics, and reporting activities. Another key feature required while developing a compliance data store is data governance. A well-defined data governance structure will help to manage audit, reconciliation, and data contract requirements across data providers and consumers.

- **Ensuring data suitability and enrichment consistently**

  While data quality and data store are important building blocks for data strategy, it is also equally important to meet ongoing data requirements such as new data elements required by detection models or additional data required during investigation or reporting. Continuous data quality checks, uniqueness of records, and a controlled data reconciliation process to ensure minimal data leakage are all important practices to be followed in order to sustain high quality solution landscape backed by solid data strategy. Data enrichment is the process of enriching data required to feed into compliance systems as well as enriching the output to be shared with compliance analysts working on the investigation process. Creating a robust data enrichment process is essential for the initial development of compliance systems and to capture data about customers, transactions, and more.

2. Providing a unified view of financial data

FIs have developed various IT and business processes over a period of time to counter financial crime activities and manage regulators and customer expectations. At the same time, the creation of new channels and avenues for customers to transact is also compounding the challenge. FIs, therefore, need to have a unified view of financial crime across the organization. The following are a few essential aspects to consider for enabling a unified view of financial crime:

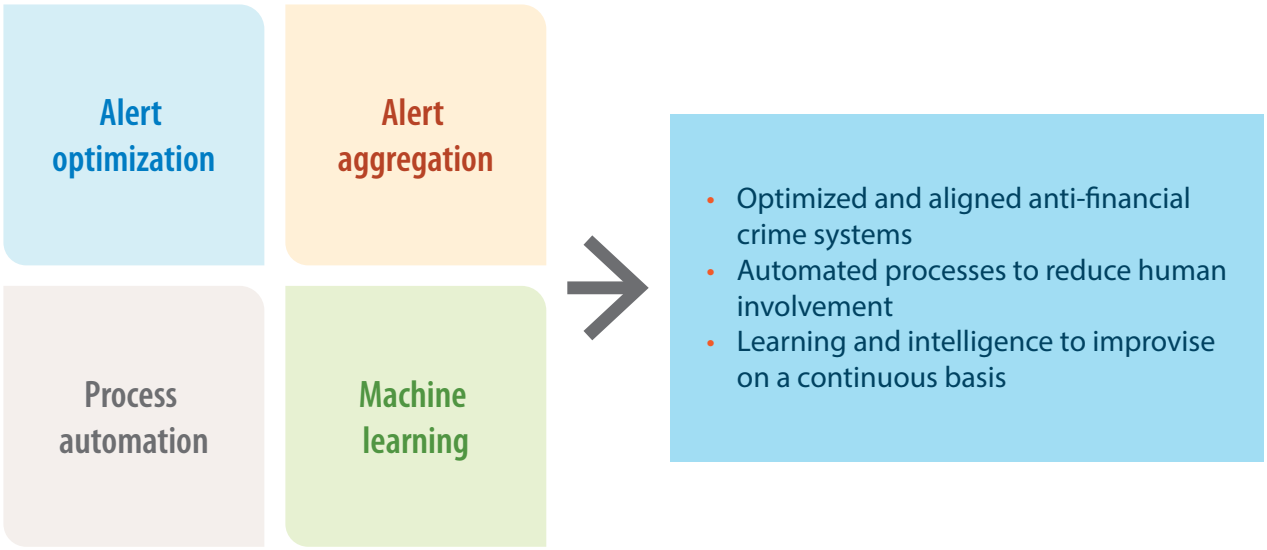
- **Holistic risk profiling of customer:**
  Customer risk profiling is a process to define risk profile of customers of a financial institution. Risk profiling is typically an automated process considering customers' financial and non-financial data and external sources of information about customers' past history. The customer risk profiling process should take into account not only customer relationship and transaction history, but also customers' suspicious activity history. It is important to connect various financial crime systems with customer risk profiling systems and processes, while arriving at a risk profile. Higher accuracy in risk profiling of customers can lead to robust compliance detection and prevention processes.
- **Enterprise-level financial crime case management:**
  Enterprise-level case management of financial crime can help in multiple ways. It could help reduce business operations cost by providing a single unified platform to financial crime business operations, instead of working through various case management systems resulting in operational overhead. With a holistic view of customers' suspicious activities and alerts, FIs can take accurate decisions on cases and prevent financial and reputational losses. A centralized platform can also enable reporting as one of its key features in meeting regulatory requirements. There is an increased level of interest from FIs now to consider this strategy. Clients are taking a mixed approach of either buying out-of-the-box solutions or configuring workflow-based tools to address this requirement.
- **External intelligence:**
  A serious attempt by FIs, with assistance from regulatory authorities, towards sharing intelligence on suspicious activities can go a long way in preventing financial crime activities. Publicly available KYC information should also be leveraged as external information, while creating customer risk profiles.

3. Optimizing data by leveraging analytics, automation, and machine learning

The compliance process to detect and prevent financial crime requires intense human effort and manual processes for case investigation and alert management. Despite numerous advanced technology measures, business operations have not seen signs of cost reduction and optimization. The primary reasons are:

- Multiple system lookups are required for data collection and analysis during the investigation process
- Experience of dealing with financial crime cases and human judgment is still the most important skill utilized by FIs
- Unavailability of uniform platforms to investigate and optimize processes

It is recommended that FIs adopt a multi-pronged approach to address the following:



Alert optimization

Alert optimization process comprises applying advanced analytical techniques to enhance the alert output of financial transaction monitoring systems. It is expected to reduce false positives generated by systems and hence reduce operational costs of financial crime business process management. There are various analytical techniques used in alert optimization including statistical analysis of generated alerts and its correlation with the segmented data. Proven techniques of above the line and below the line testing help to arrive at the right thresholds to be configured in financial crime systems. This entire process is iterative in nature and should be executed during initial implementation and on an ongoing basis while introducing new financial crime rules or models or any regulatory / business changes.

Alert aggregation

Alert aggregation is grouping of alerts based on customer, logical entities, or party. Aggregation will bring in all related alerts together in a group and assist in the investigation process. Grouping or roll-ups could be done by various parameters like customer type, risk profile of jurisdiction, transaction type, etc. Alert scoring is another related technique which enables prioritization of generated alerts based on predefined parameters and helps in assigning high prority alerts to queues with swift action plans. This can help streamline business operations and follow the right business and regulatory priorities.

Process automation

Process automation or robotic process automation (RPA) is a very good technique widely used in the banking and financial services industry to automate processes. Customer complaints management, loan origination, and client onboarding process are some of the examples where business operations have benefitted by RPA. From a compliance perspective, the key areas which are being automated are KYC processes, exit management, alert data collection, and reporting. RPA tends to automate repeatable tasks, which can follow a predefined decision process and does not require human judgment. Areas like AML case management or complex fraud are difficult to fully automate. However, part of this process could be automated to collect data, look up related systems, and perform certain reporting functions.

Machine Learning

Application of machine learning is gaining visibility in compliance systems. It's an ability of systems to learn from data and find new insights and reapply the learnings back to the system. A typical example of machine learning is when we get promotional offers on e-commerce websites based on our past purchase history. In the world of compliance there are areas where machine learning adds a lot of value. For example, machine learning can be applied for pattern recognition by finding insights from data and applying it to financial crime detection models thereby making detection systems more accurate. Another area where maching learning can be leveraged is in analyzing alert data and applying learnings in taking automated and informed decisions on alerts. This takes into account past decisions taken on alerts, customers' transaction history, and thresholds defined to take automated decisions on alerts.

Way forward – what should financial institutions do?

- Create robust compliance systems and processes to combat financial crime. This can significantly reduce risk, optimize cost, and improve efficiencies
- Build a strategic solution which has a solid, scalable, and lasting foundation over which complexity can be added on with time and increasing regulations
- Utilize the solution to supplement the growth in business as well. For example, while analyzing transaction patterns during investigation of a particular customer, unique insights about activities can be revealed
- Find innovative ways to reduce business operation costs
- Involve senior management to build a culture of compliance. Business strategy, product design, sales targets, and performance evaluation should not have objectives and incentives that are in conflict with the AML program objectives
- Ensure high-quality, aggregated data across all LOBs and product lines – this is a prerequisite
- Use analytics to derive intelligence from compliance data and further refine and fine-tune the overall process
- Upgrade the skills and knowledge of the compliance team to comprehend newer payment methods, digital channels, financial products, evolving economy and financial systems (cryptocurrency, blockchain, etc.), and regulations. Similarly, the software solution should be reliable, scalable, and adaptive to new trends such as machine learning, which have the potential to significantly improve the compliance landscape.

About the Author

Amit Khullar

Industry Principal, Financial Services, Infosys

Amit Khullar works as Industry Principal with the Infosys Financial Services vertical and is responsible for practice management for the Risk & Compliance domain. Amit comes with 17+ years of experience in managing banking, and risk & regulatory compliance initiatives with financial institutions globally. He is responsible for solution consulting and delivery management for transformational initiatives across various Infosys clients.

References

- *CEB Tower Group report on Enterprise Fraud Management April 2016*
- *PwC Paper - On the case: Mitigating emerging financial crime risks through enhanced case management*
- *Tower Group Research 2016*

For more information, contact askus@infosys.com