Capgemini

Real-Time – Know Your Customer (RT–KYC)

AI powered, data centric

Table of contents

PART 1

Real-Time KYC and smart technology

What makes KYC real time – Domain and technology enablers

High-quality real-time data management is becoming a mandate for KYC. These building blocks allow companies to save time and costs, achieve regulatory-driven accuracy, and allow organizations to better understand their customers' behaviors and financial needs.

Effective use of appropriate enablers and an organization's technology readiness are the key drivers to allow organizations to make-real time KYC possible for themselves and their customers.

KYC: Current landscape and challenges

According to Financial Action Task Force (FATF)'s recommendations, any customer due diligence (CDD) program of a financial institution should consist of four basic principles:

- Verifying customer's identity using reliable independent sources
- Taking reasonable measures to verify the identity of the true beneficial owners
- Obtaining intelligence on the purpose and intended nature of a business relationship
- Conducting ongoing due diligence throughout the relationship to ensure that transactions are in sync with an institution's knowledge of the customer, its business, risk profile, and its source of funds.

Traditional (manual) KYC, which relies on individuals in front, middle, and back offices to complete the client due diligence, may not fulfill the FATF objectives due to limitations of the conventional ways of conducting CDD and introduces the following challenges:

1. Data latency due to heavy dependency on external data to conduct KYC and multiple external channels/vendors currently being used
2. Heavy costs related to operational expenses managing manual KYC processes and KYC information stored in multiple systems
3. No data quality check with manual KYC forms or processes
4. Inability to take care of changed profile dynamics or risk factors quickly, applicable for an individual or legal entity
5. Non user-friendly interfaces while performing KYC, requiring more time to complete simplistic processes which can otherwise be handled with automation or by using artificial intelligence
6. Time latency in reviewing and verifying customer data due to a lot of manual intervention and subjectivity
7. Customer risk not being updated frequently and heavy reliance on manual processes for risk assessments and scorings
8. Lack of ability to utilize customer activity in risk models
9. No golden record for KYC, resulting in operational inefficiencies and negative customer experiences (multiple risk classification may exist and KYC updates may be requested multiple times).

(Source: Thomson Reuters, KYC compliance – The rising challenge for financial institutions, 2017)

Real-time (instantaneous) KYC does help in addressing these challenges by applying a common principal of real-time, quick request and response during most of the client onboarding sub processes. The ultimate goal of real-time KYC is minimal data (response) latency during the following processes:

- Customer and account origination
- Interactions with external data providers and rule engines: Ability to absorb and utilize most current data from government/semi government/market data providers quickly allows organizations to absorb and utilize the latest customer intelligence for KYC purpose
- Parallel processing for multiple sub processes (e.g. credit, legal, tax due diligences) contained in the overall KYC process to reduce go-to-market time for new account creations
- Streamlining of the KYC update and collection process at the entity, sub-entity, and customer level
- Data Availability: Ready availability of common data (for example, document library availability across applications to all users) across application to reduce the time taken by each business user to wait for inputs for their own respective processes.

Common principles which allow financial institutions to move towards the goal of real-time KYC as identified below not only act as driving forces but also as pillars for establishing a successful, real-time KYC set-up:

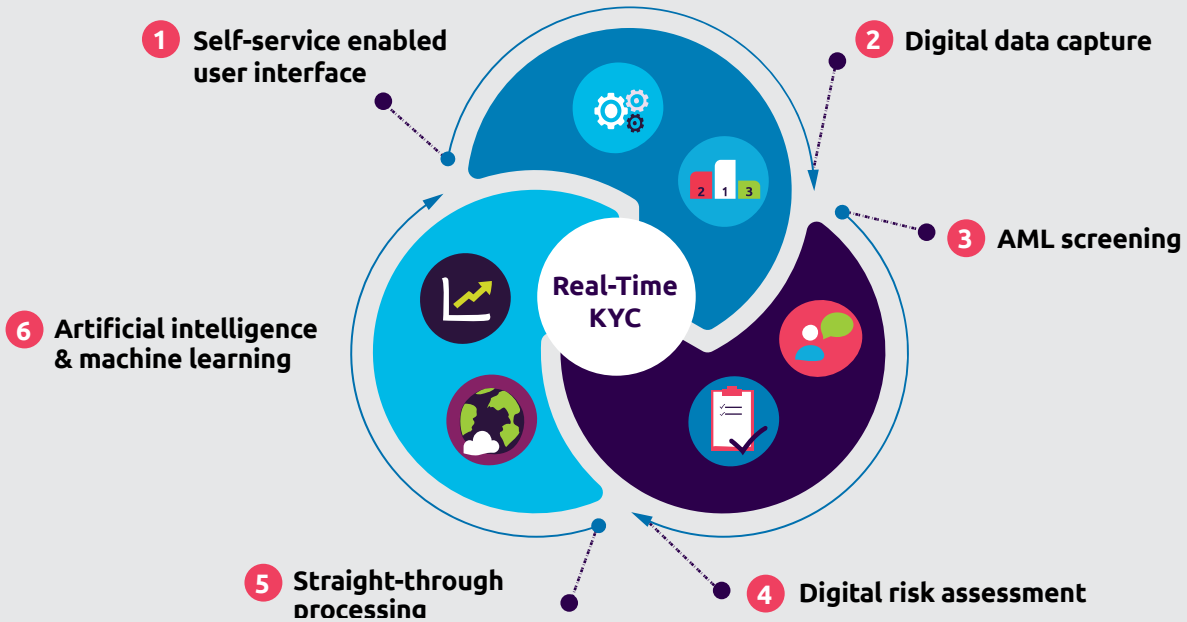
- Increased use of digital technology to achieve the goal of reduced go-to-market since “digital” means skipping the status-quo and long user queues in manual KYC collection and allowing automation of KYC processes
- Decentralization of entire KYC process by using KYC utility-like features promoting re-use and reducing re-work on pre-verified identifiers
- Inculcation of a data-centric approach than a data-driven approach for data governance
- Use of future-oriented technologies like DLT (Distributed Ledger Technology) for effective re-use of existing client information

Hence, in order to achieve the universal goal of a quick, minimal-latency-oriented (i.e. real time) KYC, we have identified technology enablers below allowing any financial institution to achieve the desired end objective most effectively.

Real-time KYC: Enablers

A robust framework for digital KYC relies on a range of building blocks specific to workflow, data automation, document management, risk profiling, anti-money laundering (AML) screening, and effective dashboards for complete user control.

Figure 1. Real Time KYC Enablers: Bird's Eye View



1. Self-service enabled user interface

A digital application or portal with a secured URL reduces the overhead and time to process manual submission of KYC details. The solution can also verify data in real time as the process is being completed so that, before it reaches the master data source for due diligence purposes, it is up to date and system verified. Sales, KYC analysts, and other back-office operations, including legal, credit, and tax, can thus be assured that they have sufficient and verified artifacts for their authenticity, allowing them to move quickly during a client due-diligence exercise.

2. Digital data capture

When opening a new account, the ability to perform as much of this digitally without the need to visit a branch is imperative in this age of digitalization. Technologies like mobile image processing with deep convolution biometric face-matching technology can be used for verifying photos with those on identification documents. This will also help financial institutions stay ahead as we move into 5G networks and truly embrace the use of mobile technologies and digitization.

Built-in forensic screening in the app can also help eliminate forged documents. Identity documents like passports can also get classified and authenticated against digital record databases and relevant information can be used in populating KYC systems using Optical Character Recognition. Continuing the theme of digitalizing, financial institutions that offer e-signature capabilities can provide better frictionless and streamlined digital processes.

Displaying data digitally and in a user-friendly manner is also of the same importance. A new KYC suite of products should ensure all users working on a client's KYC have a common view of ongoing activities, red flags, negative markers, and the recent/future activities upfront in the form of a digital dashboard. Views can be customized based on who is reviewing it.

3. Screening and digital surveillance

A robust AML screening platform coupled with digitization of KYC process allows organizations to substantiate the customer due diligence (CDD) or enhanced due diligence (EDD) process using screening results which are obtained through:

a. Round-the-clock monitoring of the sanctions lists
b. Using stringent research and inclusion criteria
c. Increasing breadth of taxonomies and keywords used in search
d. Establishing linking between associated subjects to identify criminal networks and associations
e. Integration to data providers.

4. Automated risk analysis

It's important to eliminate or reduce manual interpretation as much as possible to create a data-driven decision-making process. This way, when a client profile is augmented and enhanced, FIs should be able to automatically arrive at an accurate risk score that will drive the appropriate level of due diligence required using a risk-based approach.

Automatic categorization of clients into low, medium, or high risk using sophisticated rules engines gains a clear view of the scope of risk for the organization from a financial, regulatory, and reputational perspective. This, coupled with internally developed risk engines, can also bring an organization's specific risk factors into play, thus confirming a robust risk assessment specific to a client base catered by a financial institution. The usage of data, its quality, and risk-scoring models can also help identify unknown risks and learnings from the customer behaviors which should feed into the risk assessments rating.

Automating consumption of this data via third-party data providers such as LexisNexis, World-Check and RDC, further reduces the need to ask customers for information and adds independent verification to the process.

Also, a key aspect for a successful AML screening while performing real-time KYC is Centralized Data Management. If a customer already has a relationship with a financial institution, it should be possible to re-use and re-purpose this information. The ability to integrate with key internal systems should make this a distinct possibility. Also, where multiple accounts may exist in different countries for the same customer, Centralized Data Management can help provide a single customer view.

The role of Digital Market Surveillance in AML screening is also vital. False positives are costly affairs. Surveillance-area turnkey solutions using customizable rules engines can enable banks to decide preset thresholds for alerts, increasing credibility of digital surveillance.

5. Straight-through processing

A straight-through process (STP) implemented at the organizational level brings in additional efficiencies with reference to capturing and storing required KYC documents, their integration with Document Management Systems, integration with screening/monitoring systems to block or freeze transactions which are possibly fraudulent (substantiated by enhanced due diligence during KYC, also flagging exceptions for manual review). STP confirms that data captured at various stages is reviewed frequently, thus substantially reducing the possibility of incomplete KYC data or mitigating the risk of data-quality issues and accuracy of data.

Also, integration into a series of third-party sister systems and bank-owned internal data repositories is a must to enable a streamlined KYC processes and approach real-time efficiency.

- Automating the consumption of this data via third-party data providers and/or KYC registries and utilities further reduces the need to ask customers for information and adds an independent verification to the process.
- The ability to integrate with key internal systems should encourage a single client view at group level, leading to the possibility of reusing and repurposing client information within the different entities of a single group and between its business lines and geographies.
- API connections into CRM systems can provide the visibility that relationship managers need when onboarding clients for real-time information about applications.

6. Artificial intelligence and machine learning

AI ensures that a KYC verification is performed in real-time. Use of natural language processing (NLP) and machine learning (ML) allows it to read huge amount of information in any language, thus increasing efficiency of the KYC process as a whole.

It helps improve the KYC process by:

a. Automating client risk profiling and associated additional due diligence
b. Precise identification of beneficial ownership of complex legal structures
c. Precise interpretation and link analysis to produce accurate representation of the legal entity structure
d. Workflow automation wherever essential
e. Pattern detection in the vast amount of data received, which is key for regulators to identify anomalies and use this process into the tuning of alerts which will help reducing false positive and increase the quality of alerts learnt from various patterns and customer behavior.

Figure 2. Deeper understanding of how each of the enablers or components of enablers are typically leveraged across the value chain of the KYC process.

KYC Process	Digital Lever	Benefit
Digital data capture	Biometrics/RPA/DLT/OCR	Real-time identity verification
Customer due diligence	AI/ML/NLP, link analysis	Reduce time to complete CDD
Enhanced due diligence	AI/ML/NLP, link analysis	Reduce time to complete EDD
Customer screening	RPA, AI/ML/NLP	Decreased false positives
Risk assessment	AI/NLP, RPA, link analysis	Realistic and current risk calculation
Reporting	RPA	Efficient Internal & external reporting
Periodic reviews	RPA, AI/ML/NLP	Effective data streamlining processes
Record keeping	RPA	Effective data archival, retention & disposal

PART 2

Collaboration to enhance RT-KYC

Making real-time KYC possible: Collaborative approach

Financial crime and compliance are still highly manual work streams. More banks are considering a collaborative approach to accelerate and bring more efficiencies to their KYC processes. Distributed ledger technology (DLT) can be expected to help overcome most of the challenges faced.

Data and policy standardization and collaboration as necessary steps for a scaled real-time KYC

Information asymmetries are caused by information silos. Information silos are created when specific data about the client is fragmented across different databases, limiting a comprehensive overview. Therefore, many want to harmonize requirements across different regulatory regimes, aiming at developing standards to create efficiencies and improve compliance. However, this does not fully solve costly duplicative processes that occupy most of the manual workloads. Hence, the need exists for an infrastructure that allows for trustful and secured data-sharing whilst safeguarding data privacy and all the necessary traceability required by compliance. Such a platform shall support straight-through connectivity between organizations, with integrated workflows, while being able to adapt easily to the evolving regulatory demands. To set it up successfully, it is essential to converge the KYC policies and IT infrastructures of the involved stakeholders. This can only be achieved through deep collaboration between involved parties.

There are different kinds of potential collaborations to improve overall compliance and bring additional real-time capabilities to KYC processes, each of them related to a specific use case.

- **Collaboration within a financial institution** to harmonize processes between the different entities and business lines of a financial institutions and set up a proper infrastructure to enhance straight through processing and compliance monitoring at global/local levels. The main use case for such an internal collaboration is the setup of a company-wide KYC platform.
- **Collaboration between financial institutions** to agree on harmonized and mutualized datasets and processes to favor better compliance. Those collaborations can be done at a global and/or local level. The main use case for this kind of collaborations is the setup of KYC utilities.
- **Collaboration with regulators** to enhance financial-institution auditability and reporting-by-design. This kind of collaboration can both be applicable for single company use cases and multicompany initiatives.

These collaborations and their related use cases can be considered independently from each other or interrelatedly for more efficiencies.

Design assumptions for a successful collaborative infrastructure:

In order to co-operate whilst using sensitive data among different parties, there must be a certain degree of trust among stakeholders. For this to work, the target infrastructure must deliver the following:

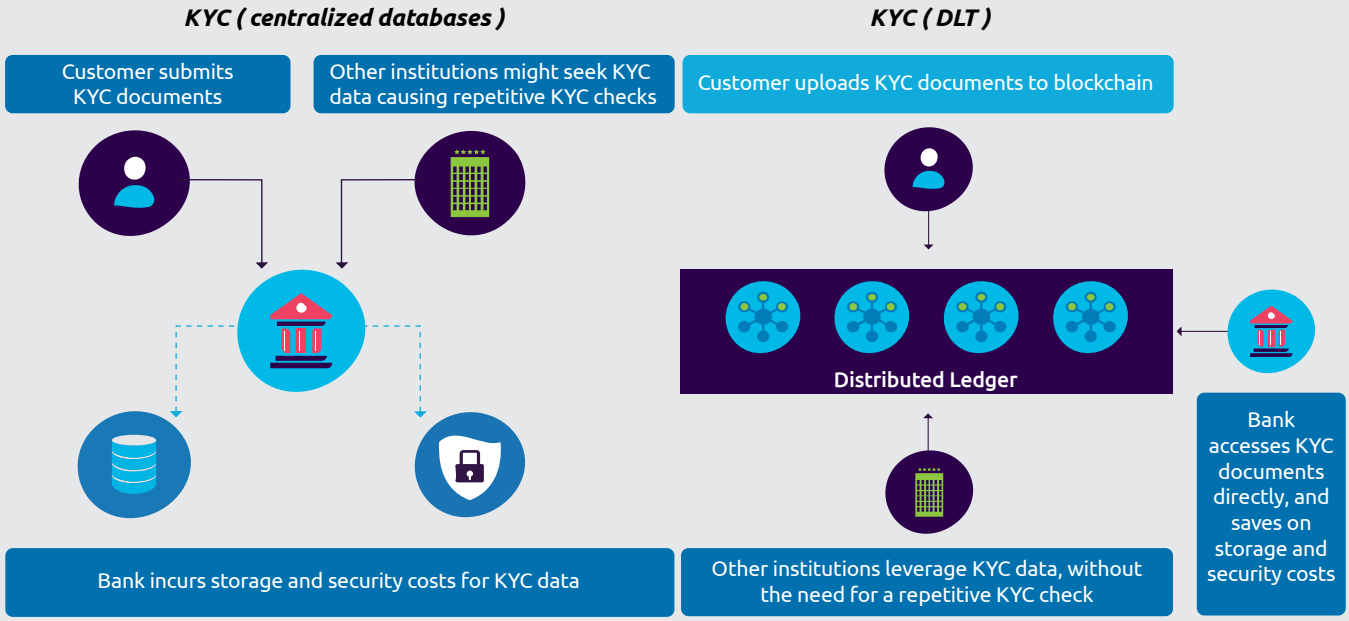
- **A governance framework**: This framework enforces the rules of engagement among stakeholders. It should stipulate how independent actors who interact are aligned on a certain level of input quality. Furthermore, it must enlist mechanisms that incorporate privacy laws and only provide access on a need-to-know basis.
- **Efficiency by design:** To ensure efficiency, the infrastructure shall rely on the best technologies to favor automation and Straight-Through Processing by design. Also, the use of "golden sources", provided or approved by regulators or trusted sources, will improve the level of confidence in the data and facilitate the setup of procedures focusing on use cases that require true focus.
- **Futureproof:** Where a governance framework guarantees a set of rules cultivating trust, the design framework should be focused on the robustness and interoperability of participants' systems. In contrast to legacy systems that were robust and non-standardized, a new infrastructure must maintain some flexibility at its core. In other words, it is necessary for the infrastructure to provide seamless integration with all the solutions that could be required by participants' compliance. From a technological perspective, it should be compatible with all new innovations and RT KYC enablers, such as automation and AI.

How can DLT help with real-time KYC

The technology that seems to fit perfectly to these core design assumptions and use cases is DLT, of which the most famous implementations is blockchain. According to the International Telecommunication Union, a specialized agency of the United Nations that is responsible for issues that concern information and communication technologies, a distributed ledger is one that is shared, replicated, and synchronized in a distributed and decentralized manner. DLT enables users of the distributed ledger to reach agreement and record information without relying on a central trusted party.

DLT systems can be public and permission-less or private and permissioned. In a private and permissioned system, access to the network is restricted to a limited number of participants and different levels of permissions can be assigned to network participants. This type of DLT system seems to be the most suitable to enterprise use-cases such as KYC, where confidential data is shared among participants.

Figure 3. Distributed Ledger for KYC



Source: Capgemini Financial Services Analysis, 2019; Capgemini Retail Banking Top Trends report, 2019

A DLT- based solution for KYC would bring the following benefits to the financial institutions:

- **Greater operational efficiency**, by enabling the inclusion of secured and properly organized data-sharing workflows into the overall KYC digitized process flows. As it targets multi-actor workflow, DLT can reach a new generation of Straight-Through Processing efficiency.
- **Full data ownership and control**, by providing each participant a way to decide and manage how data is shared among them. The consent mechanism, which can be automated to target real-time processing, is strengthened by the ledger capacity to prove how and when sensitive data has been accessed and used.
- **Tamper-proof auditability**, by providing a way for participants to show regulators and auditors the process they went through. Instead of proposing an incomplete collection of logs, financial institutions are able to de-risk themselves by providing an indisputable and exhaustive list of proof-points.

Use cases for DLT in KYC and compliance

According to a study published by the European Commission (https://ec.europa.eu/digital-single-market/en/blockchain-technologies), a DLT solution would be perfectly adequate for the following KYC-related use cases:

1. KYC platforms powered by DLT

The benefits of an internal KYC platform relying on a DLT solution are threefold. It improves data quality since information that is uploaded on the network must adhere to the consensus protocol ensuring quality of input. Secondly, it improves data-sharing since it allows each department to update information about the client and control the way it is shared with other participants. Lastly, it facilitates the delegation of KYC tasks to preferred locations, participating in removing redundancies and increasing efficiencies and real-time processing across departments. (Source: https://www.finextra.com/blogposting/18610/the-role-of-blockchain-and-dlt-in-e-kyc-utilities)

2. Multi-participant DLT-powered KYC utilities

A KYC utility based on a DLT solution would provide the same benefits as the internal KYC platform but would not limit it to internal processes of a single group. Also, the implications of additional participants could increase efficiencies and lower redundant manual work. Consequently, it would enhance transparency among the participating institutions and substitute information silos with a single point of truth accessible by all participants on a need-to-know basis. Thanks to the transparency inherent to the technology, a DLT-powered KYC utility could enhance its mutualization and verification capabilities and bring more efficiencies to its services. Also, such a DLT-powered KYC utility could facilitate the setup of daily monitoring process on KYC profiles, specific to bank needs, and enable proper real-time alerting of any material changes and associated results to the participating financial institutions.

3. DLT-based reporting systems

Current reporting systems could be enhanced by a DLT solution, thanks to the high auditability of DLT systems. This could be done for example by connecting regulators and auditors to the DLT network and enabling banks to share through this secure channel any necessary proof of work in real time. These immutable records will be game changers in the ease of administration and quality of regulatory oversight and compliance.

PART 3

Data as the nucleus of KYC

Data-management discipline and analytics

Data-management discipline and analytics are the nucleus of KYC. This section explains data strategy as a key consideration and nucleus for KYC solutions, and provides an overview of a methodology that can be used to implement data-centric KYC solutions

What makes the data-management discipline more critical for KYC solutions?

Data-management discipline is the key element for analytics. It is critical to have consolidated enterprise-level data management discipline to arrive at reliable decisions that enable analytics. The greater the data discipline, the more reliable and accurate are the analytic outcomes, which helps business make the right decisions.

In the financial world, KYC has many components, depending on usage of KYC and business context. The most relevant KYC workflows are client identification, verification, transaction monitoring, sanction-screening, black-list monitoring, suspicious activity reporting, and maintaining information for the workflow of KYC, as mentioned above. Data quality and accurate data of the above workflows are very critical to run flawless operations of KYC.

Data plays vital roles at all stages of KYC. Failure to collect accurate and relevant information at early stages impacts efficiency and adds costs and delays the entire process of KYC.

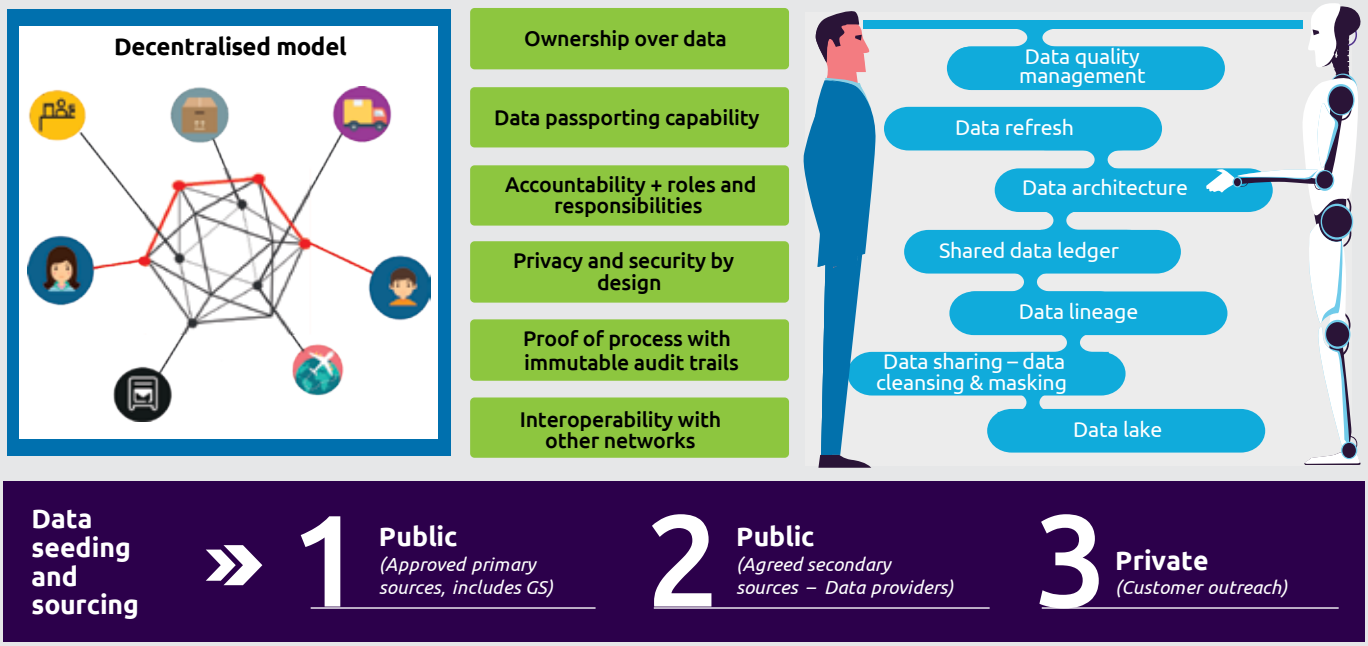
The data strategy and its alignment with an organization's vision statement is paramount for impactful business outcome. An impactful enterprise data strategy focuses on data-management discipline, enabling the ancillary factors – like data governance, data quality, data integrations, ETL meta data, data migration, and extracted data – to act as building blocks covering data criticality in more holistic ways to deliver the best results.

Data discipline is vital to get the intended results for KYC solutions and to make it more cost effective and current. Each of the data-discipline components have compliance to adhere to, for building stronger KYC solutions.

The value of data is in the information it contains, and its use of data management discipline is key for relevant and reliable analytics.

Figure 4. AI powered data-driven real-time KYC

Solution structure – data-driven



Data-driven KYC or data-centric KYC solutions

The world of big data is magical, and even more so for KYC solutions and development. KYC solutions are shifting gears from data-driven to data-centric, often leading to lots of efforts in harmonizing data before meaningful results are produced in data lakes.

The value-chain movement of an organization takes place based on the amount of experience it possesses in data-driven solutions, thus allowing it to move towards a data-centric organization.

Real-time KYC solutions require a data-centric approach: The decision between data-centric versus data-driven is more relevant when we are moving KYC solution towards real time. Application-centric KYC solutions are not able to meet demands of real-time KYC solution because of the core modules' inability to adopt changes which are required to be economical, faster, and efficient in reducing the documentation and information asks for KYC frameworks.

Deriving data value from AI and ML: Real-time KYC solutions rely on smart technologies such as AI and ML to make real-time connections to KYC legal entities, linkages, identifiers, due-diligence documentations, watch lists, anomaly detection, and the critical workflow of KYC processes across global linkages.

Conclusion:

The rules of the game are changing. Data relevancy, recency, and accuracy are becoming the most important aspects for regulatory agencies to measure the accuracy of KYC programs within organizations.

As we see more and more organizations being fined in 2019 due to inability to track crimes early and promptly, moving towards real-time KYC is a must. All organizations have an increasing need of making real-time KYC an integral part of their ecosystem due to regulatory pressures to be as accurate as possible.

Also, the recent trend has shifted towards a more collective approach for compliance, with notable efforts to standardize and harmonize KYC data and policies, both internally and at the multi-financial-institutions level. One thing has become clear: there is a growing need for KYC IT infrastructures to connect seamlessly across business lines and/or geographies to bring more effectiveness and real-time capabilities to current systems.

Technology enablers including self-service user interfaces, digital data capture, and effective use of artificial intelligence and machine learning, as well as a collaborative infrastructure consisting of future proof, efficient technologies, including DLT, is a necessity in making the KYC process real time in a true sense.

Strategic and mature data management discipline at the enterprise level is a backbone which is a common thread irrespective of which technology, tools, and process flows one leverages for making client due diligence more robust and error free.

An early adoption of real-time KYC by each organization is necessary to avoid cost overheads and inefficiencies associated with continuing with conventional client due diligence and thus necessitates detailed study of all enabling factors, allowing an organization to achieve the end objective of real time in a true sense.

About the Authors:

Mathias ROS is a senior project manager and business analyst for Capgemini Business Services. After 10 years working for large financial institutions in various projects and business domains (financial crime, credit risk, payments), he is now focusing on the design, build, and operation of new solutions to connect business ecosystems and enable secure data sharing by leveraging blockchain technology.

Mangesh Gholap is a senior consultant and is a lead analyst for the Financial Crime & Compliance Center of Excellence at Capgemini. He possesses 13 years of experience in financial risk and compliance arenas, acting as a Program Manager and Business Analyst for various banking clients, leading many IT consulting and transformation initiatives across various clients at Capgemini, and is also a member of various organizations including the Association of Certified Anti Money Laundering Specialists and the CFA Institute.

Manorama Kulkarni is Director of Financial Crime and Compliance, Capgemini. Manorama is also an alumni with legal, academic, and banking expertise spanning 20 years in business process management and strategic roles.

About Capgemini

Capgemini is a global leader in consulting, digital transformation, technology and engineering services. The Group is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms.

Building on its strong 50-year+ heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. Today, it is a multicultural company of 270,000 team members in almost 50 countries. With Altran, the Group reported 2019 combined revenues of €17billion.

Learn more about us at

www.capgemini.com

People matter, results count.

Capgemini