





The Path to **NEXT-GENERATION** KYC-as-a-Service Solutions

 Are your current KYC/CDD operating model and solutions really bringing the expected value?

 The emergence of collaborative infrastructures for KYC/CDD is paving the way for new operating models

 The next-generation 'KYC-as-a-Service' solutions





Executive Summary

Financial institutions are undergoing radical transformation, challenged by the digitization of processes, the platformification of business ecosystems, as well as data protection and cybersecurity issues. The COVID-19 pandemic has brought to fore these concerns and in this challenging environment, risks need to be managed efficiently to prevent operational and reputational damages, while complying with increasingly complex regulations and policies.

Fundamentally, these challenges point to the need to foster trust within business ecosystems, and between business partners. Building trust is primarily based on the reliable identification and verification of business identity, as a cornerstone of any business relationship.

Referred to as “Know Your Customer” (KYC) / “Client Due Diligence” (CDD) processes in the financial industry, these processes are driven by strong regulatory requirements, with geographic specificities, and are part of the overall measures taken by governments and financial institutions against financial crimes.

In this white paper, we set the task to address these challenges and analyze the following:

- **Data and technology solutions for process and cost efficiencies:** In this context, the emergence of new technologies such as APIs, data analytics, intelligent automation, and distributed ledger technology is bringing new levels of cost efficiencies and extended connectivity, when combined with proper supervision and controls.
- **External and internal data sharing:** We believe that enabling secured data sharing between properly identified business partners throughout their respective ecosystems contribute to laying the foundations of a trusted business environment for improved efficiency, better compliance, and more sustainable business relationships.
- **New operating models:** After assessing managed services and utility models, it leads to new operating models where KYC/CDD processes could be processed extensively “as-a-Service”, based on better controls, enhanced data quality, and tamper-proof traceability. These new kinds of ‘KYC-as-a-Service’ operating models will bring extended capabilities to financial institutions, to overcome current KYC/CDD challenges and open the door to new flexibilities in the way they manage KYC/CDD processes without compromising on the quality of the surveillance.

Capgemini’s recognized experience and proven capabilities in the design and set up of highly efficient KYC/CDD solutions are dedicated to supporting your transformation journey through all its necessary steps, from strategic design to product implementation, maintenance, and operations, jointly with our KYC technology partners.



Arindam Choudhury

Global Head, Banking and Capital Markets, Insights and Data, Capgemini Financial Services



Preeti Malik

Head of global Risk and Financial Crime Compliance, Banking and Capital Markets, Insights and Data, Capgemini Financial Services

INTRODUCTION

Banks and other financial institutions have been trying to better **'know their customers'** for decades now. Both for regulatory requirements and to protect their business against financial crime, banks have been pursuing deeper and more intimate knowledge of their clients. KYC and operations teams have had the challenge of managing the pressure coming from clients, front offices and regulators, supporting business as a partner, while ensuring compliance and protecting the bank. But the process has always been an arduous and labor intensive one, one where complexity is continuously increasing.

In parallel "As-a-service" has become a mantra in technology over the last decade, as on-premise solutions have been replaced increasingly with cloud-based ones. **Know Your Customer (KYC)** and **Customer Due Diligence (CDD)** operations continue to evolve as many clients are looking for solutions to bring costs down to sustainable levels, while improving compliance and providing better customer experience.

In this paper, we explore new and evolving strategies for banks to perform their KYC and CDD activities more effectively and efficiently, including how to extend KYC operations to next-generation "as-a-service" models.

In our findings, we uncovered some consistent concerns among our clients, including :

- How do we reach operational efficiency in KYC while simultaneously improving customer experience?
- How can standardization, collaboration and technology be leveraged to tackle the key challenge of siloed information?

In our view, trends in technologies have led to the development of next-generation **'KYC-as-a-Service'** solutions, adaptative to each bank's specific framework and able to accelerate their transformation. These solutions can enhance a financial organization's ability to orchestrate its entire ecosystem at play – including BigTech, RegTech, FinTech and other technology and business partners – while also enabling advanced compliance services and effective utilization of internal and external data.

The never-ending costs and burdens of KYC/CDD compliance

The average financial institution spends \$60 million per year on KYC and CDD and \$58 million per year on client onboarding. Some global institutions spend more than \$500 million annually on these activities.¹

While those processes are still perceived as very complex for customers, recent studies have shown that the potential cost of losing even a small percentage of new customers due to complex manual KYC processes can be as much as \$12 million a year for a large financial institution.

Also, in some markets such as trade finance, the cost of compliance is so important that it is literally deterring banks from providing trade finance to smaller companies.²

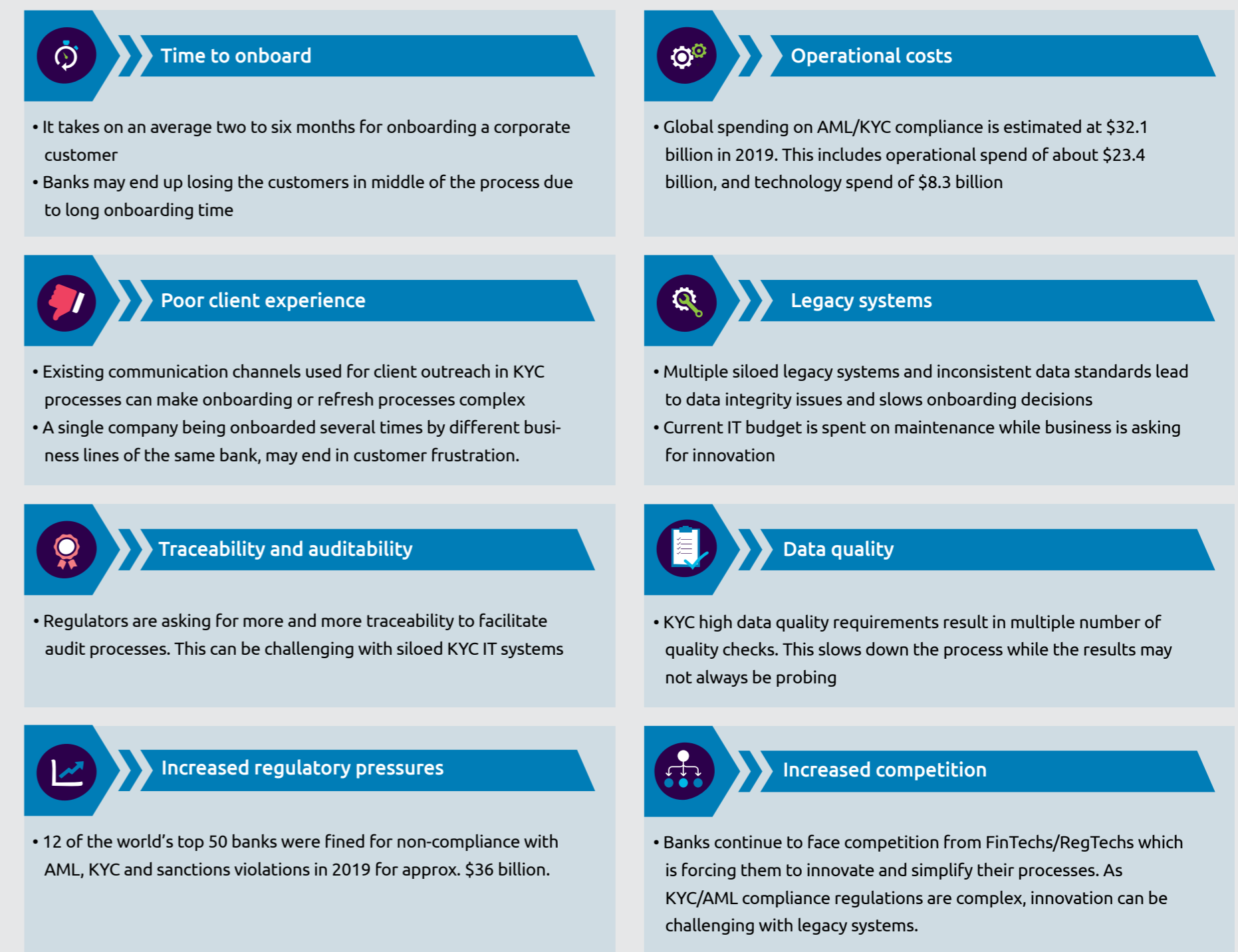
Those challenges can all be tackled by leveraging two key elements of any properly designed KYC/AML system: **data and delivery**.

At a moment where COVID-19 has shown the pressing need for advanced digitization, the ability for financial institutions to enhance customer digital interactions and propose adaptative products while maintaining compliance surveillance appears more important than ever. In this context, greater levels of cooperation should be encouraged, bringing competitive advantage to financial institutions that will take the lead.

¹. Know Your Customer Survey, Thomson Reuters

². Asian Development Bank (ADB) Brief, 2017 Trade Finance Gaps, Growth, and Jobs Survey

Figure 1: Main challenges for KYC/AML





Are your current KYC/CDD

operating model
and solutions really
bringing the expected value?



Recent surveys have shown that an estimated average of **80 percent of banks' regulatory client data costs come from maintaining data.**

To financial institutions, data poses a challenge and a solution at the same time. Because insights are only as good as the data that comprises them, data quality is always an issue. However current procedures and systems are proving inadequate for acquiring and maintaining quality data. That is why, efficient data-driven process design can lead to enhanced operational efficiency and regulatory compliance.

Data quality is the cornerstone of any efficient KYC/CDD system

Data quality is something any large enterprise must address. However, there are some fundamental roadblocks that must be overcome to ensure the cleanest possible data. These include:

- Inadequate controls over required data fields and sources
- Inadequate methods of obtaining and/or maintaining current and correct customer data
- Multiple systems and repositories with no single "Golden Record"³ of information.

To tackle these issues, technology and digitization should be used to improve data quality and ultimately bring better compliance and foster customer experience.

KYC/AML processes are all about assessing the validity of a customer. If the data available to describe a client's identity, activity, or behavior is missing or altered, then the whole assessment is fouled, resulting in longer or repeated processes and potential false positives.

For the best results, the KYC/AML data lifecycle must be secure and reliable from end-to-end -- from data collection to data maintenance -- and leverage existing technology to achieve straight-through-processing. At the data collection level, better data quality can be enhanced with the use of trusted sources. This is accomplished by enhancing client outreach channels for data that needs to be obtained directly from clients. It can also be leveraged from trusted sources of data (or "golden sources") for any other data collected to complete the profile.

Figure 2: Data management core issues in KYC/CDD processes



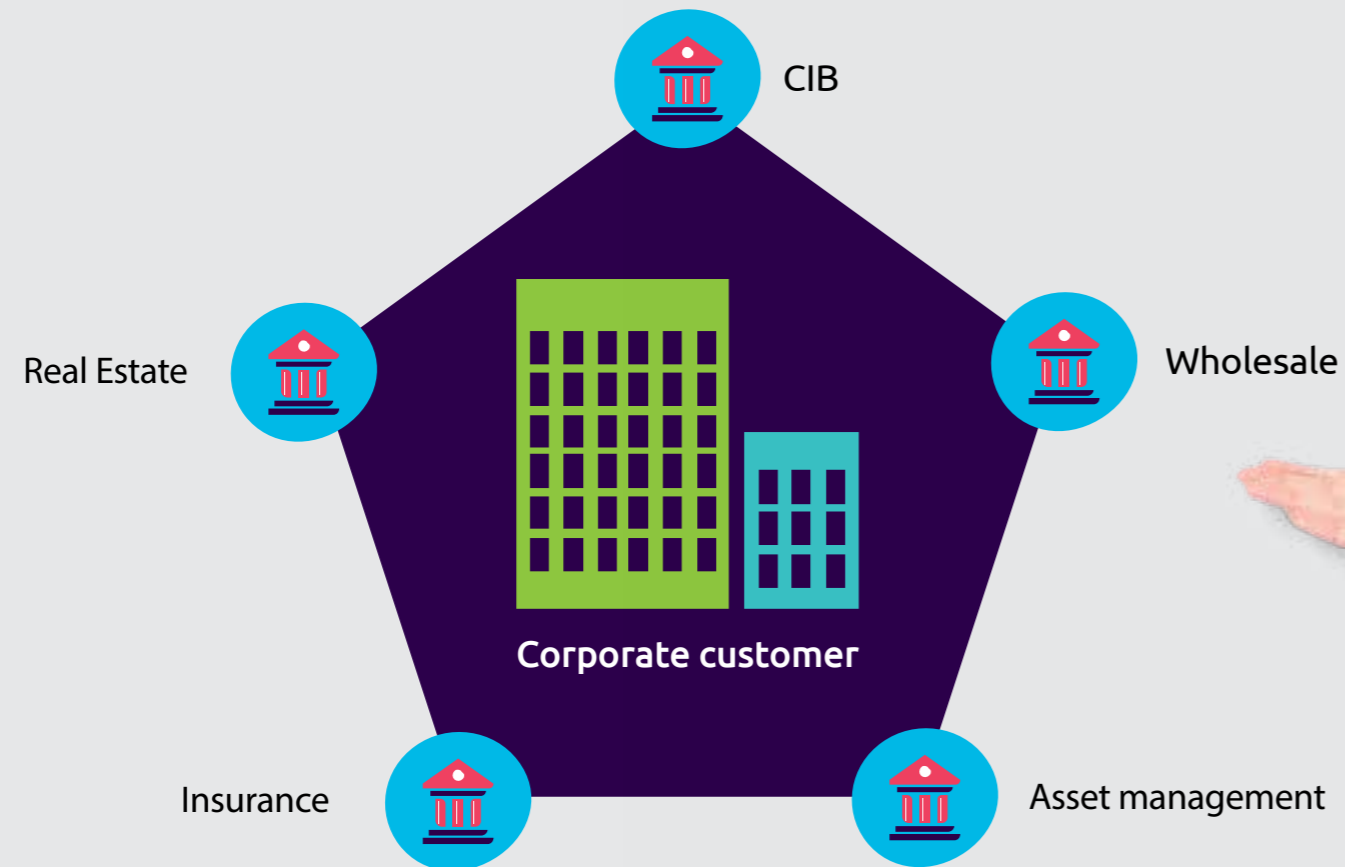
While large amounts of data collected for KYC/AML purposes will be unstructured (i.e. adverse news, organizational structures, etc.), the use of advanced tooling such as Intelligent Automation and Optical Character Recognition (OCR) can be used to create structure and reduce inefficiencies. These tools can be used to conduct third-party searches, gathering of information and enrichment of customer profiles. Further, they will enhance many other traditionally manual processes. In the end, they complement sourcing capabilities and improve data reliance, and ultimately, overall data quality.

³ By « Golden Record » we understand a single, complete and up to date overview of all available data from the Bank's systems on a customer, available to all bank entities and businesses.

Once collected, the quality of data can be maintained by building infrastructures that enable straight-through-processing and automation, ensuring the data is not altered by manual mistakes and remains up-to-date. Also, verified Legal Entity Identifiers, "LEIs" such as global LEIs, can dramatically simplify entity identification across different lifecycle stages.⁴

Finally, it is also important to have a system that holds a single "golden record" of a financial institution's clients in order to give their KYC department the tools and insights required to process information quickly and effectively on a periodic basis. **Coupled with modern automation technologies, such an internal KYC platform would allow financial institutions to build data-driven approaches to create more efficient onboarding or periodic reviews as well as creating a holistic or 360° view of their client base.**

Figure 3: "Golden record" of a client enables a single customer view across various business lines, departments, geographies etc.



⁴ <https://www.gleif.org/en/lei-solutions/mckinsey-company-and-gleif-leis-and-client-lifecycle-management-in-banking-a-u-s-4-billion-beginning/>

Putting the client experience at the core of KYC

According to recent industry surveys, **38 percent of customers** stated user experience as the most important criterion when choosing a financial relationship. Further, **26 percent** stated that easy onboarding is essential. On average, during the onboarding time, corporate clients are contacted approximate 10 or more times and asked to submit as little as five and up to 100 documents (either directly or through external sources). One of the key expectations from the customer for financial institution is to make onboarding processes easy, efficient and provide better customer experience.⁵

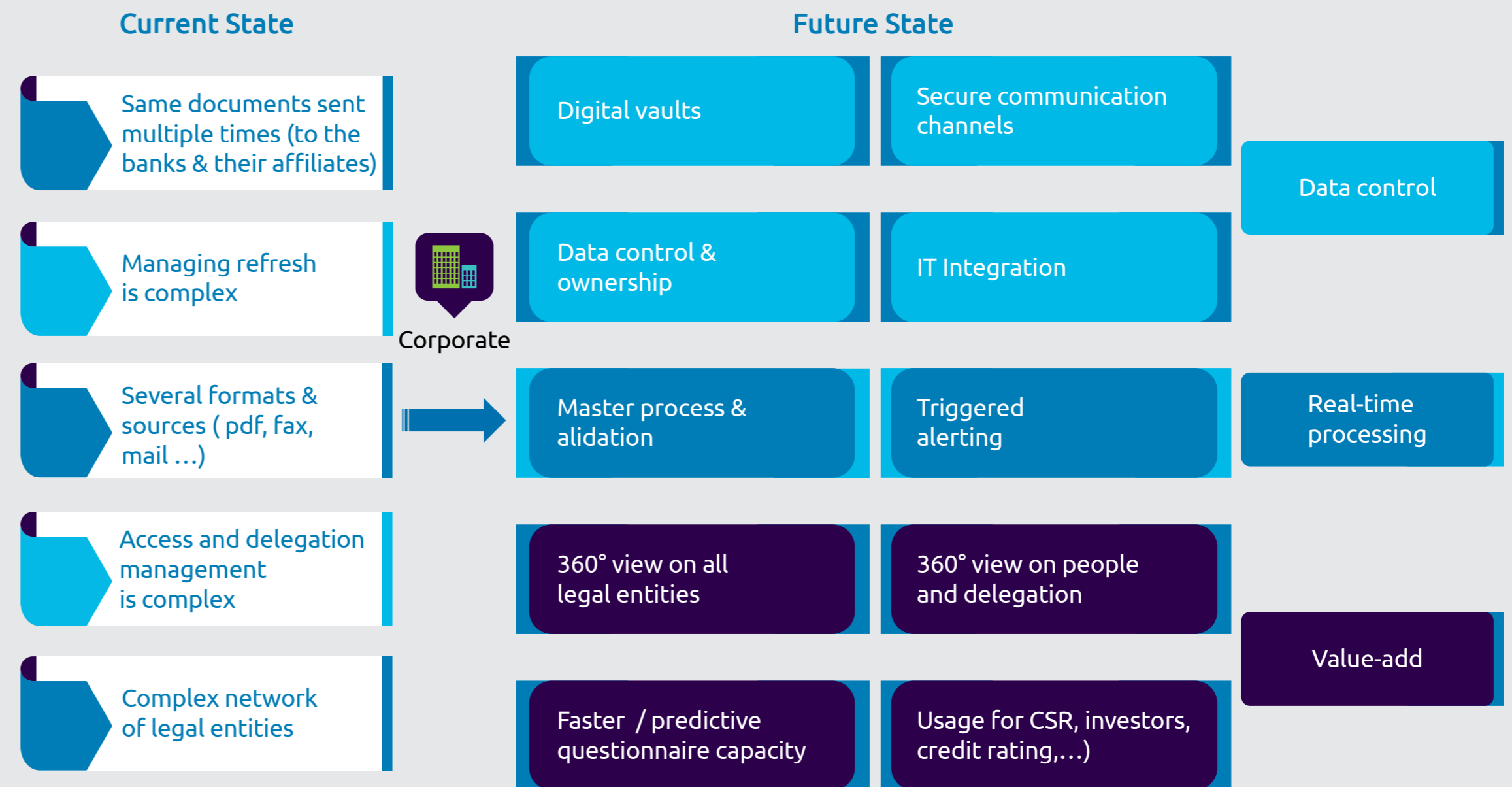
In KYC/AML processes, client interactions mainly take place during the account opening process or in the context of ongoing trigger- or event-based due diligence tasks.

By using digital strategies such as customer portals and support for multiple channel communication, the friction inherent in gathering the necessary customer documentation can be vastly reduced.

A main driver in creating elevated customer experience is an elaborate onboarding strategy. The customer should have his entire onboarding and review cycle in one efficient channel, without too many points of contact. It is core to understand a customer's needs and use new and appropriate service design techniques to cater to that need.

⁵ EACT Briefing, Focus: KYC, 2019

Figure 4: For corporate customers, KYC experience could be greatly improved





Also, strategies to foster the creation of value for the customer should be considered and encouraged. For example, as client outreaches for data and document collection are redundant, banks or their partners could offer customers a way to manage their data and draw tangible value out of it.

Recently, two initiatives provide good examples on how banks could enhance their corporate clients onboarding experiences:

- **JP Morgan Data Once** offers a data-driven solution for JP Morgan group⁶, with very high rates of customer satisfaction. Within the Data Once solution, the banks' customers provide their data through a single channel. The data is then accessible and transferable across the various products and geographies of the group. Customers are then able to visualize the use of their data and the status of the existing KYC requests, providing them with as much control as possible over their data in the interactions they could have with the bank and its partners.⁷
- **SWIFT KYC Registry for Corporates**, launched end of 2019, offers corporates a secure interface to manage and share their KYC data with their banking partners across the globe.⁸ Created with a working group of large-scale corporates and financial institutions, this centralized registry acts as a trusted third-party to facilitate data collection and maintenance for Banks. This program has received support from large institutions such as BNP Paribas⁹, Phillips or Unilever.¹⁰

In both cases, the solutions have been more widely integrated into the Banks digitized KYC systems and enhance customer through accelerated onboarding times.

⁶ <https://www.euromoney.com/article/b18fq8n85h5ssh/banks-versus-fintechs-2-tension-builds-with-regtech-innovation>

⁷ <https://www.jpmorgan.com/country/US/EN/ts/client-service-and-implementations>

⁸ <https://www.gtreview.com/news/global/swift-opens-kyc-registry-to-corporate-users/>

⁹ https://cib.bnpparibas.com/our-news/swift-kyc-registry-goes-live-for-corporates_a-33-3312.html

¹⁰ https://www.swift.com/news-events/news/enabling-smoother-know-your-customer-kyc_processes-for-corporates





Enhancing customer experience through digitization and automation

The amount of time it takes to onboard a new client can vary from days to months, depending on the level of digitization a financial institution has set in place.

Digitalization and automation are key in assuring better compliance with AML regulations by reducing manual errors, but also to simplify the onboarding process and provide a better experience.

The development of intelligent automation, cloud computing, artificial intelligence (AI), biometrics, distributed ledger technologies etc., is enabling important capabilities to achieve compliance by improving data quality and maintenance all along the KYC value chain.

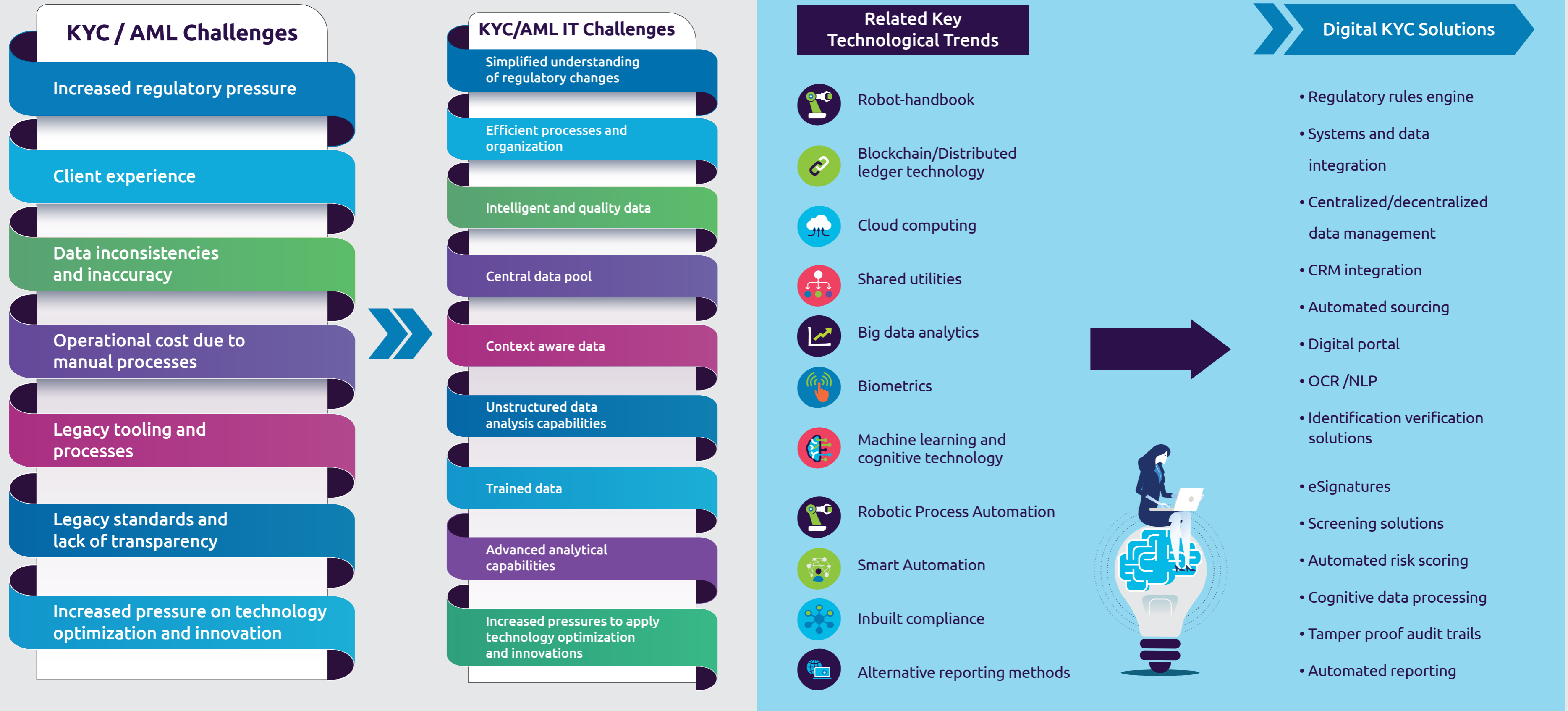
By using APIs, digital and automated tools can be connected to each other and to many other solutions, including external company data providers, screening solutions and internal bank repositories. Moreover, it provides the ability to integrate them into the end-to-end workflow, enabling a proper orchestration of all related KYC/CDD tasks.

In the end, the digitization of KYC processes provides enhanced customer experience through:

- Shortened processing time
- Elimination of manual errors
- Increased data quality and consistency
- Streamlined processes
- Security in the handling of customer data
- Improved auditability



Figure 5: Digital KYC/AML components overview



Standardization and mutualization to tackle information silos

To be able to deploy such a digitized KYC/CDD workflows at scale, financial institutions need to ensure that every party can share data in a format that can be easily ingested by each other.

Therefore, it requires to define a proper data governance framework along with the standardization and harmonization of the flows through which data will be processed.

Information silos are created when customer data is fragmented across different databases, limiting a single overview of the customers. This causes inefficiencies when the customer has various products or services across different departments or geographies. Moreover, the same customer can also hold multiple accounts at different banks, resulting in each institution having to repeat similar due diligence tasks and, by consequence, high levels of redundancy. More importantly, information silos are creating an important risk of failure for KYC/AML controls at global scale, as criminals and money launderers may use lacks in existing monitoring systems to find ways to finance their activities. These kinds of weaknesses have been identified in various geographies, such as the Netherlands, where an estimated €16 billion in illicit funds are known to be circulating currently.¹¹

Therefore, many institutions want to harmonize requirements and data taxonomies across different regulatory regimes. By doing so, they aim at developing standards to create efficiencies and evenly distribute controls to improve overall compliance.

Externalization to provide flexibility and enhanced services

Following this logic of digitizing and harmonizing KYC data and processes, the use of external partners is one of the key delivery models to find better efficiencies in KYC/AML processes, while benefitting immediately from cost savings due to mutualization. By providing a way to delegate KYC/AML tasks to trusted third parties, externalization can bring more flexibility in operations, especially when supported by up-to-date technologies.

KYC Utilities and KYC managed services are the current main offerings for KYC externalization.

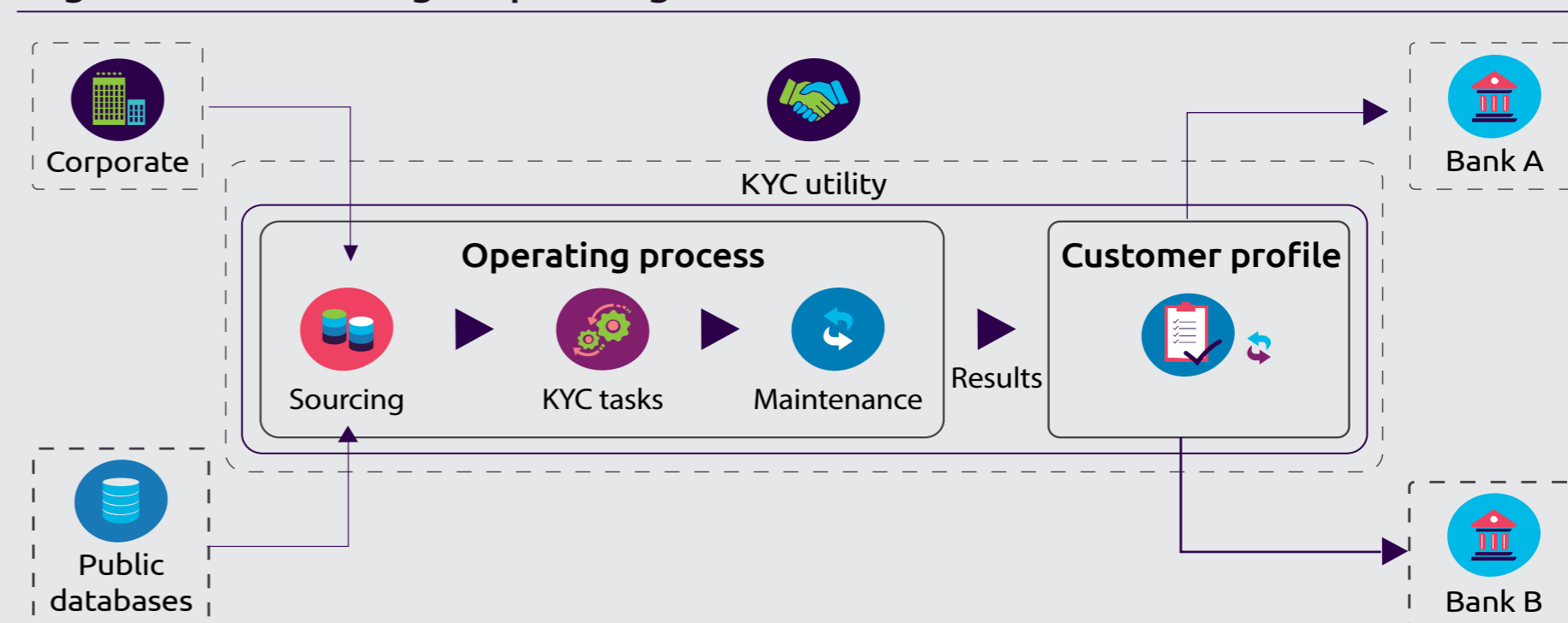
KYC utilities provide mutualized services

The first KYC utilities were introduced in 2014. They were centralized databases, controlled by a single entity and working with a certain number of partner banks to mutualize data collection and controls. Despite strong support from influential financial institutions, their success has been limited because they were mainly perceived by customers and front offices as disintermediating customer relationship, while generating legal, compliance, operational and data quality challenges to banks.

In spite of those challenges, the utility model has recently been revived as regulators have become increasingly concerned by money laundering risks in specific geographies or sectors (i.e.: trade finance). There are multiple local public-private initiatives emerging across different geographies (South Africa, the Nordics, Middle East, the Netherlands and Singapore, to name a few of them).

The main value proposition of KYC utilities is to provide Financial institutions with standard customer profiles that have been aggregated beforehand or on-demand by the utility along with the results of limited KYC tasks, like Politically Exposed Persons (PEP) or sanction screening, upon a standardized baseline.

Figure 6: Generic target operating model for KYC Utilities



¹¹ <https://www.moneylaundering.com/news/largest-dutch-banks-plan-shared-kyc-database/>



However, if mutualization can be easily obtained by leveraging public data sources, it can though be limited, as the sharing of private data sourced from data providers or bank proprietary data can be a cause for concern. This is mainly due to banks data privacy and secrecy rules or contractual agreements between data vendors and banks. This limitation could be skirted by establishing strict data sharing and liability rules between the different stakeholders of the KYC utility, preferably with the support of local regulator, and proper consent management at the customer level. Some geographies or projects even consider changing their local regulation to enable such a local platform to operate.¹²

However despite all the transparency that could be encouraged or accepted to fight financial crime, Banks may remain concerned that their customer outreach and relationship can be altered by the KYC utility, especially if it implies having some of their private financing information shared with non-regulated third parties or competition.

KYC managed services provide bespoke services

The other asset that Banks can use to delegate their KYC processes and gain benefits from it are KYC managed services. By providing banks with dedicated level of services and dedicated teams, **KYC managed services** enable wide outsourcing of a Bank's KYC daily operations with onshore/offshore models and can propose advance support to KYC remediation projects. They provide an opportunity for financial institutions to reduce manual effort across a significant portion of the KYC process, and consequently the people costs associated with completing KYC. This enables financial institutions to redeploy their operations staff to focus on more complex, high-value tasks, such as risk decision making and increasing their monthly throughput of KYC reviews.

Through centralizing the KYC process and associated cost components for multiple financial institutions, the cost of ownership is distributed across each subscribing customer, with managed services vendors absorbing the investment risk.

Consequently, when comparing KYC managed service vendors cost components to those of a large financial institution, technology and content make up a greater proportion, delivering efficiencies and economies of scale both in terms of spend and processing effort.

An analysis by Thomson Reuters demonstrated a 35-60% cost saving per KYC review on a like-for-like basis between a managed service per-record fee and in-house operations.¹³

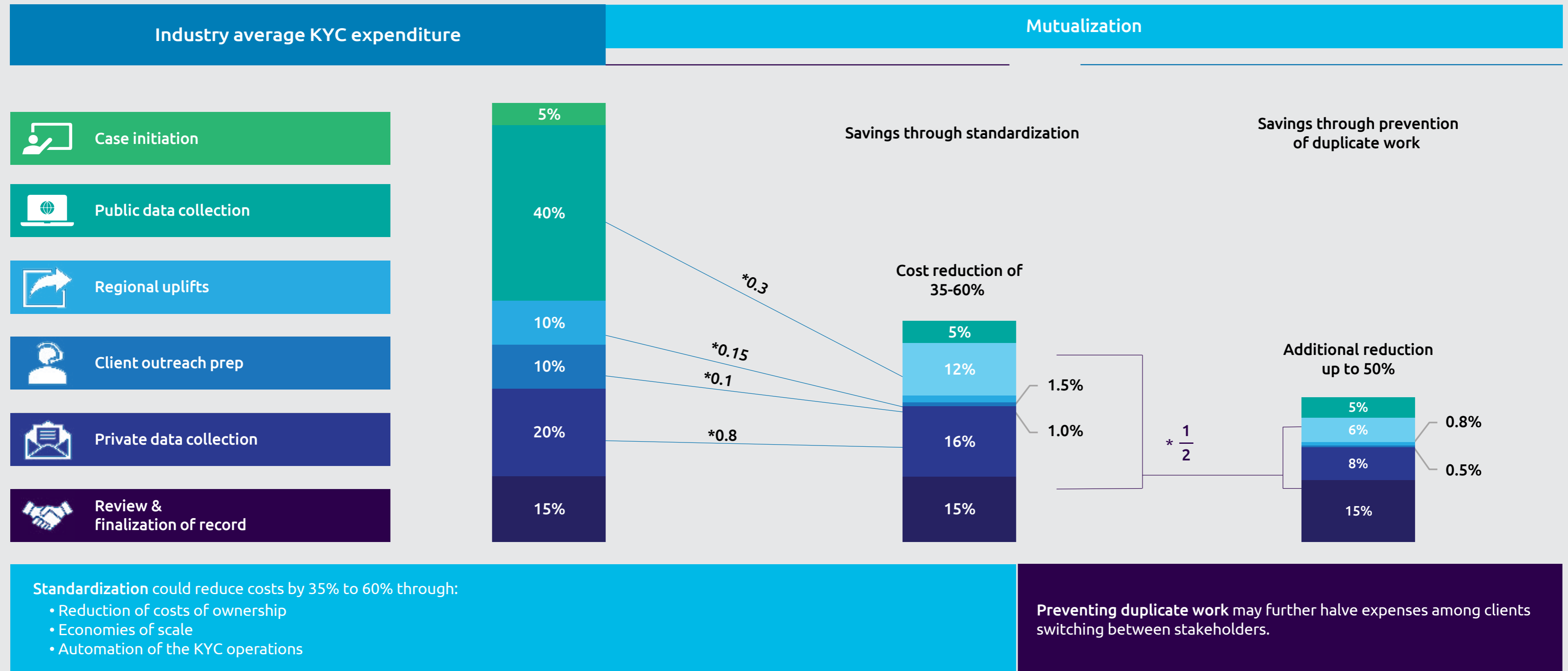
The study also shows that these savings could be greater leveraging mutualization mechanisms between partnering banks, in the context of a shared platform or KYC utility-like set up, paving the way to what an externalized collaborative '**KYC-as-a-Service**' platform could be.

¹² <https://www.financelatvia.eu/wp-content/uploads/2019/07/KYC-utility-report-June-2019.pdf>

¹³ Know Your Customer Survey, Thomson Reuters



Figure 7: Highest benefits are found in the optimization of data collection



Source: Thomson Reuters, Refinitiv

The emergence of collaborative infrastructures

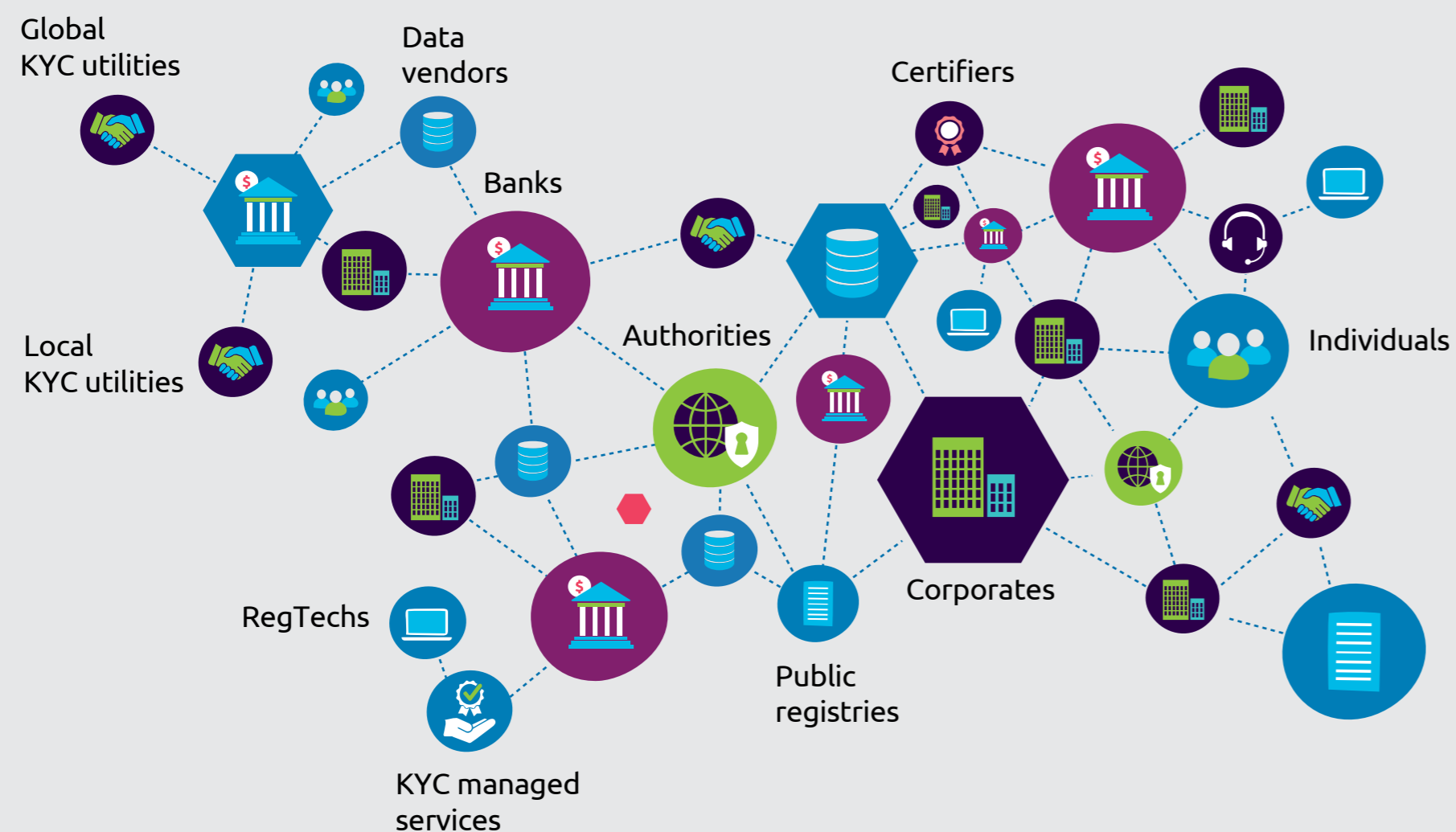
for KYC/CDD is paving
the way for new
operating models



KYC/CDD can be perceived as a network of business partners, helping each other to identify risks properly, investigate accurately, and accelerate the time to business. We have seen that KYC/CDD processes can be greatly accelerated by digitization, standardization, and mutualization. However, it remains a fragmented world where efficiencies are often limited by poor ecosystem connectivity and siloed environments, both internally and across the industry.

Recent regulatory pushes to setup local KYC registries or Shared KYC utilities point to an increasing willingness to counter the compounding effect of siloization within KYC operations. Similar pushes for collaboration, but between various entities of a single group, are also observed when local regulators warn headquarters of global groups regarding their entities' non-compliance.¹⁴

Figure 8: The collaborative ecosystem of corporate KYC



The need for such collaborative frameworks calls for the creation of **Trusted Data Exchanges**, both internally—among a group’s entities and geographies and industry-wide—among different groups sharing or mutualizing their proceeds. These platforms ensure trusted and secure data-sharing while safeguarding data privacy and other necessary compliance requirements. They also support straight-through connectivity between organizations, with integrated workflows, while adapting to evolving regulatory demands.

Collaboration for better overall compliance

Two main use cases driving the emergence of such data exchanges in the KYC space are:

- The setup of company-wide **KYC platforms**, relying on the sharing of properly referenced “golden records” of customer data and KYC profiles within the various geographies and business lines of a single financial institution, to enhance straight-through processing (STP) and compliance monitoring at global/local levels.
- The development of **KYC shared platforms** or **shared KYC utilities**, on a local or global basis, where various financial institutions collaborate and agree on a framework to share and proceed KYC data to benefit from mutualization and standardization.

In both scenarios, the key to success lies in accelerating the convergence of KYC policies and IT infrastructure of the involved stakeholders while offering the ability to accommodate some degree of bank-specific policies.





This convergence can only be achieved through deep collaboration between the involved parties. These include financial institutions themselves, along with their specific branches and geographies and their main KYC partners such as regulators, information management firms, RegTechs, and consulting firms.



¹⁴ <https://www.euromoney.com/article/b1kzfl3jxr0s1/aml-record-fine-gives-swedbank-a-chance-to-move-on>

Key design assumptions for collaborative infrastructures:

The solutions for these use-cases require a very deep level of trust to ensure all parties' data requirements are well respected:

-  **Trust in the governance of the platform** to prevent and address conflicts of interests between stakeholders
-  **Trust in the digital processes**, including their ability to ensure efficient workflows through automation and STP
-  **Trust in the auditability and traceability** of the systems for regulatory and legal purposes and to ensure, technically, the liabilities agreed by the governance
-  **Trust in the digital infrastructure** itself, including its robustness, interoperability, and scalability

Technologies to enhance and support collaborative frameworks

To attain this level of trust, various architectural choices can be considered including centralized to decentralized systems or a combination of both.

For use-cases that do not have to deal with complex data ownership requirements or data privacy rules across businesses and/or geographies, a centralized database with advanced audit-trail functions, owned by a trusted entity can fit the needs, acting as a central registry. It should also encourage connectivity and straight-through-processing thanks to Application Programming Interfaces (API). To support the necessary traceability and auditability, the database shall be reinforced by robust change tracking capabilities.

However, when it comes to managing customer data within complex banking institutions across several business lines, regions and regulatory environments, decentralized solutions are increasingly proving relevant. By allowing the setup of a **federal model**, where each connected entity owns its data and controls the way it is shared with its ecosystem, they digitally enforce accountability while offering more flexibility in terms of governance. This architecture enables accountability and responsibility of each entity while ensuring the synchronization of data between those connected parties.

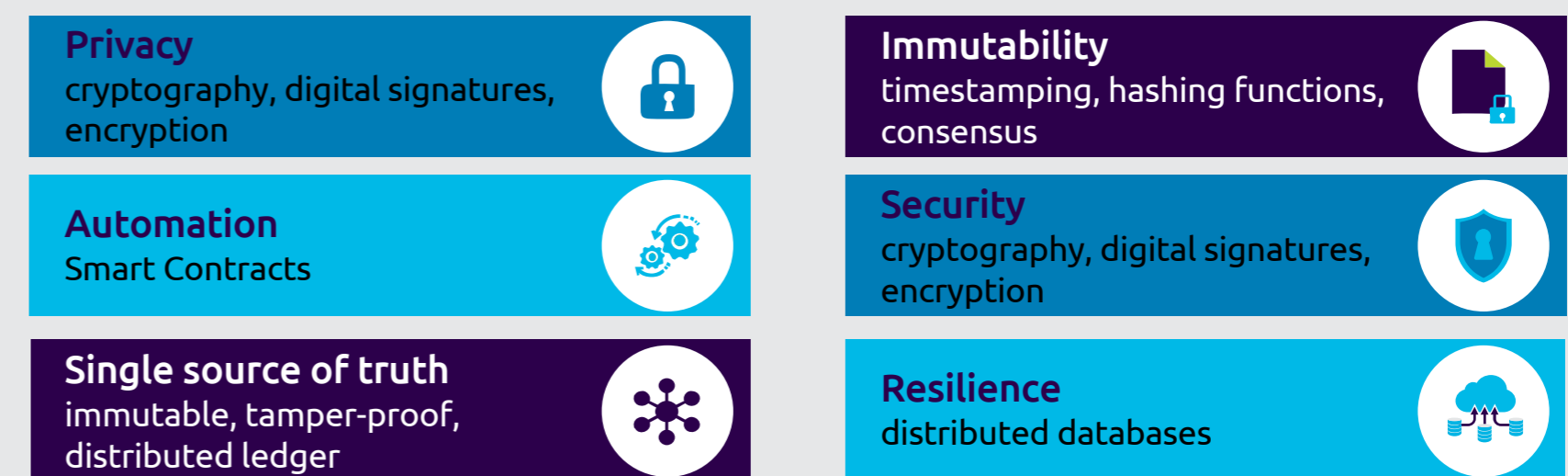
The optimal trade-off is probably a hybrid model, where a strong centralized entity operates as a control tower, while enabling each regional and business lines' hub to have its autonomy within the right overall governance.

How Distributed Ledger Technology (DLT) can help?

DLT is designed and developed to support trusted data sharing in a business environment. A distributed ledger is a "type of ledger that is shared, replicated, and synchronized in a distributed and decentralized manner"¹⁵. DLT enables users of the distributed ledger to reach an agreement and record information without relying on the central trusted party.

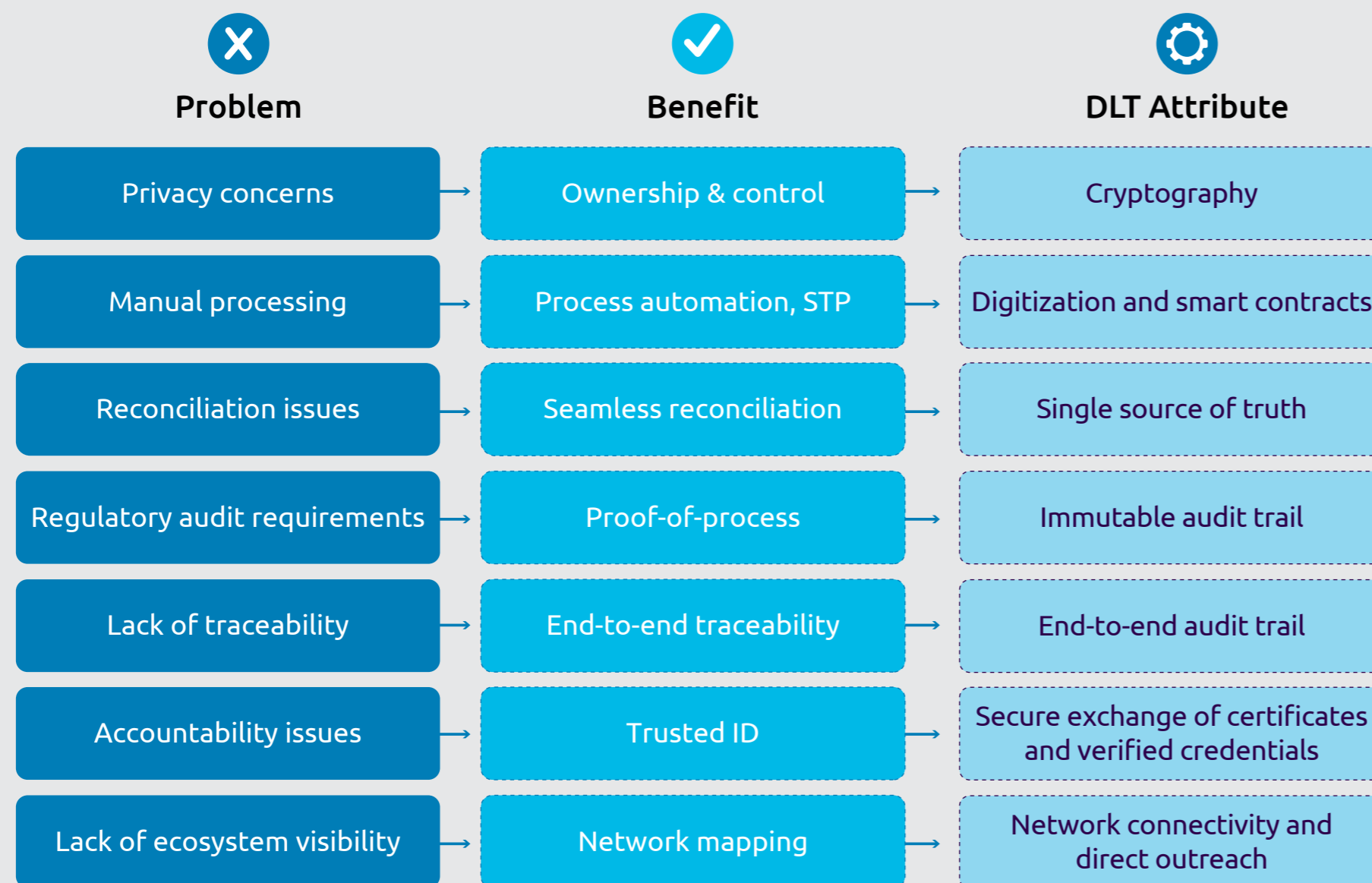
In a private and permissioned DLT, data can be shared among a limited number of participants who control the network's access and permissions. Such a DLT appears as the most suitable for enterprise use cases such as KYC.

Figure 9: Key attributes of DLT



¹⁵ [Technical Specification FG DLT D1.1 – Distributed ledger technology terms and definitions](#)

Figure 10: Problem / Benefit matrix of DLT



By relying on a DLT-based solution, financial institutions can have the following operational benefits:

- Better customer experience** by proposing new communication channels for client outreach that enhances ownership and control of customer data as well as security and privacy-by-design
- Reduce operational costs** by reaching a new generation of straight-through processing KYC workflows leveraging digitization and smart contracts
- Reduce the time to onboard** by enabling re-usability of the already collected information by other entities that could be properly traced and timestamped
- End the siloed systems** by enabling a structured solution to share KYC profiles within an organization or between organizations, that respect consent and privacy frameworks by design
- Better traceability** by enabling the end-to-end proof for all transactions during the process through a tamper-proof audit trail.

Finally, and regardless of the use case or the selected technology, the emergence of collaborative frameworks and infrastructures to support financial institutions' digital transformation calls for two types of systems. Tailor-made services, adapted to banks' specific governance frameworks, and shared/mutualized services resulting from external collaborations. Such "KYC-as-a-Service" systems should be able to propose enhanced connectivity to the wider ecosystems of KYC, including regulators as well as data and service providers to adapt to the constantly evolving regulations, technologies, and policies. Finally, they should be able to guarantee the best-of-class customer experience all along the banks' constantly evolving transformation journey.

Proof of concepts conducted in Singapore, France, and Japan by various firms demonstrated that by using DLT, a KYC platform can save the estimated cost up to 50% and considerably enhance auditability.



The next-generation 'KYC-as-a-Service' solutions

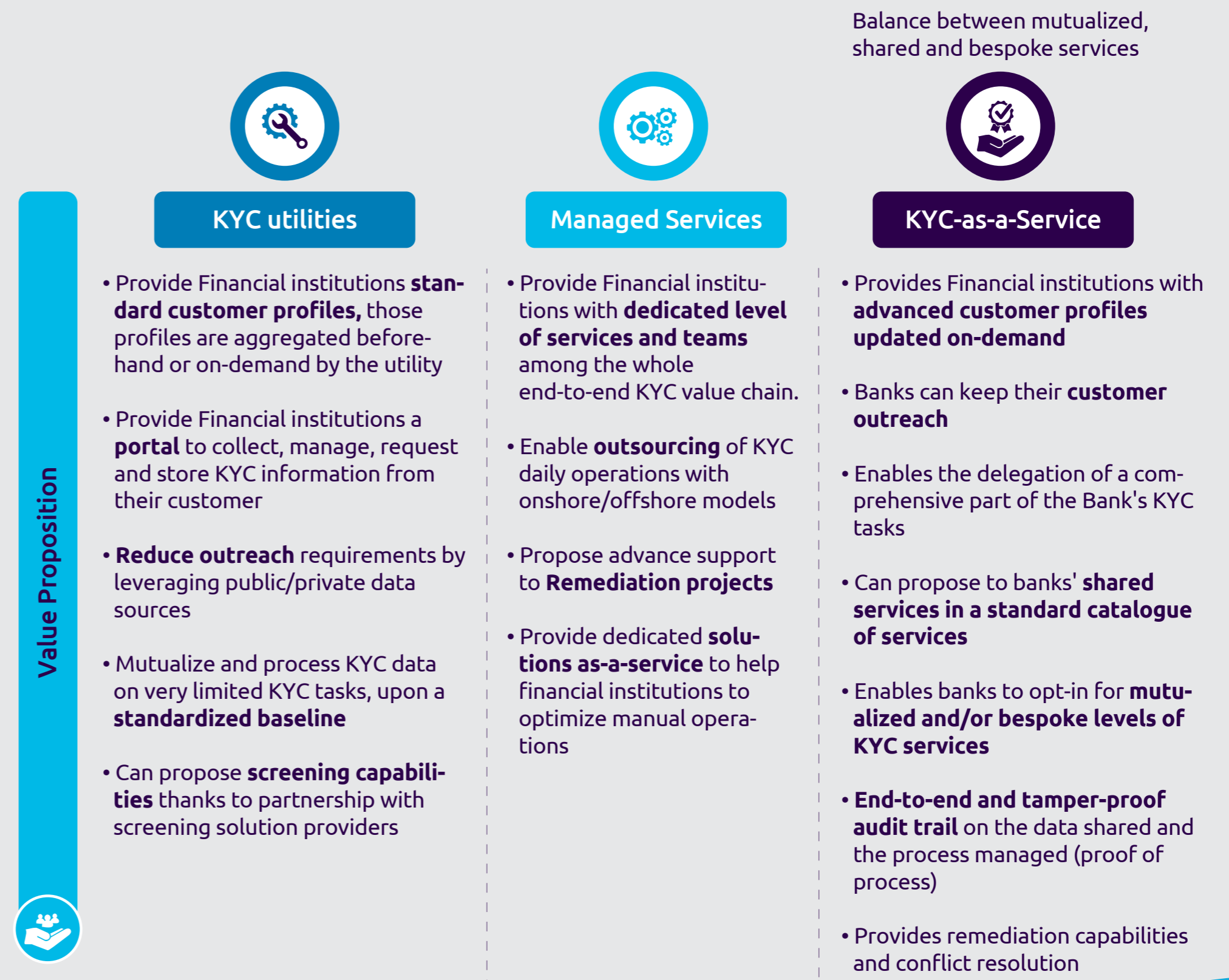


The next-generation 'KYC-as-a-Service' solutions, as we envision them, would be able to provide mutualized and bespoke services at the same time seamlessly, while ensuring great levels of flexibility both from a solution and operational perspective.

This can be also be challenging as mutualized offerings require stakeholders to agree on standards and policies as well as strict data sharing rules and liabilities when a bespoke solution offering is proposed in the place of tailor-made services specific to the banks' policies and processes.

Therefore, such solutions should have, at their core, the ability to manage segregated channels. Thus, enabling, firstly, a multi-level offering of services, from dedicated operating processes for a single bank to multiple pre-build services available to all, and secondly, agreed bespoke operating processes between business partners (i.e. local banks or different entities within the same banking group).

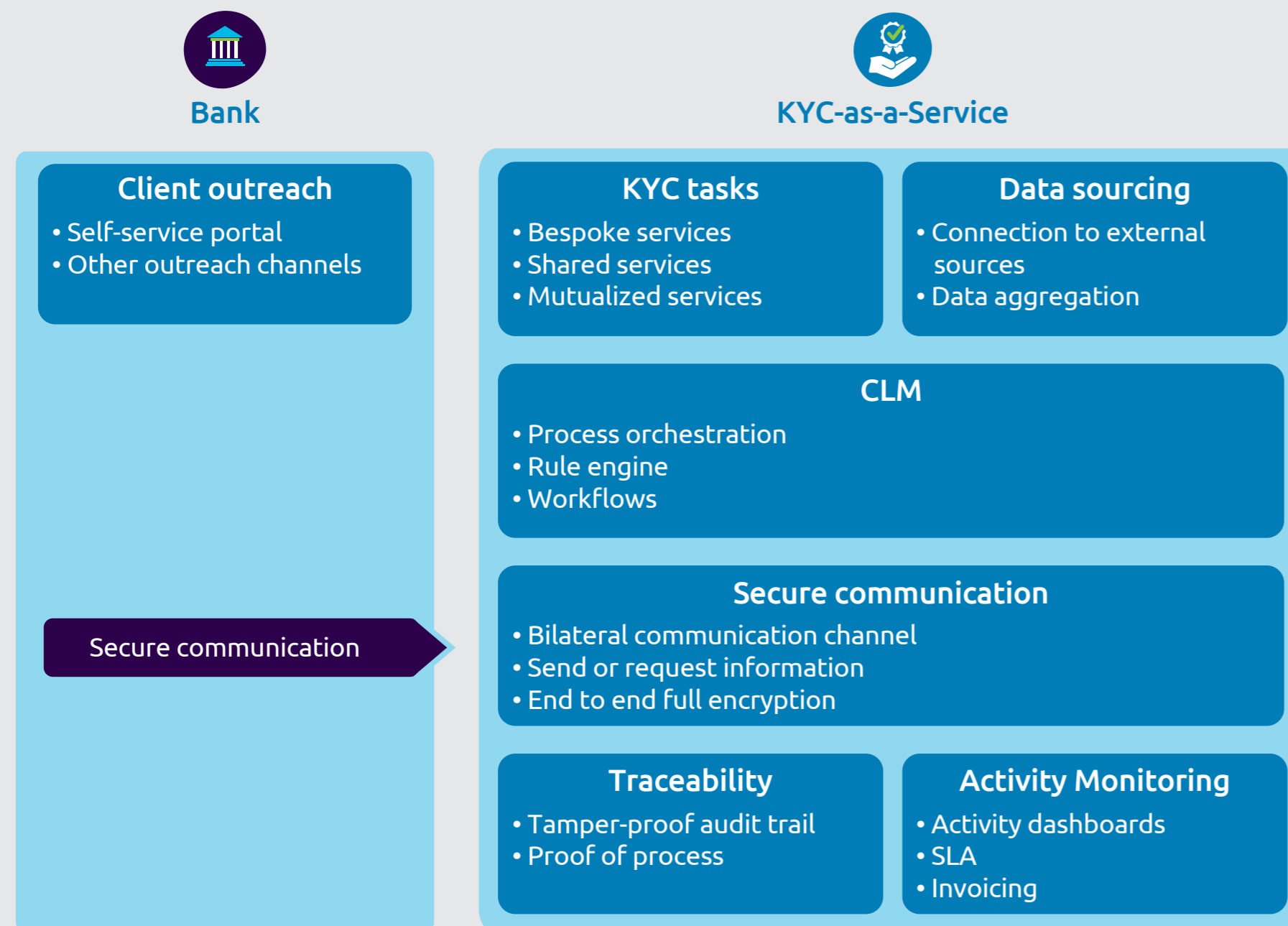
Figure 11: How KYC-as-a-Service solutions differ from KYC utilities and managed services



Key features of a KYC-as-a-Service solution

To be able to deliver such advanced level services and remain competitive, we believe that KYC-as-a-Service solutions should leverage the best-in-class emerging technology solutions and offer the following features to banks:

Figure 12: KYC-as-a-Service solution features



Direct Customer outreach: While some customers may find an advantage in managing their KYC information through a shared portal, others may prefer to share their personal information directly through their bank's channels.

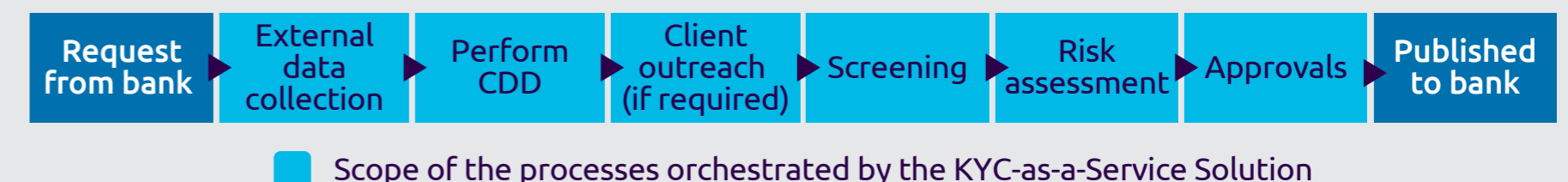


Secure communication channels: The next-gen KYC-as-a-Service solutions should leverage secure, private, and bilateral communication channels to ensure necessary 'Chinese walls' between the requirements for different banks (in case of an external KYC platform) or among the various entities of the same bank (in case of an internal KYC platform). It should, therefore, be able to guarantee confidentiality, privacy, and banking secrecy as needed. This secure communication channels should be used between involved parties to request or provide information and should ensure that privacy is respected between parties. It should, therefore, favor peer-to-peer communication and provide the necessary end-to-end encryption levels, which is one of the benefits of leveraging Distributed Ledger Technology (DLT).



Efficient KYC workflows orchestrator: The 'KYC-as-a-Service' solutions should rely on a workflow solution to properly orchestrate the end-to-end KYC process delegated by the bank. This solution should be able to build and manage customer profiles, based on customer information and regulatory requirements, as well as to ensure full compliance with risk and regulatory obligations throughout the process flow. It should also be able to trigger KYC tasks for data refreshes and ongoing due diligence processes, and therefore preferably embed a rule engine to help define applicable regulations and risk levels per customer profile, in line with the users' policies. Finally, the workflow orchestrator should provide the solution with a data model upon which any necessary baseline should be propped, enabling further interoperability with any existing data providers, verifiers, or existing registries.

Figure 13: High level scope of the processes orchestrated by the KYC-as-a-Service solution workflow engine



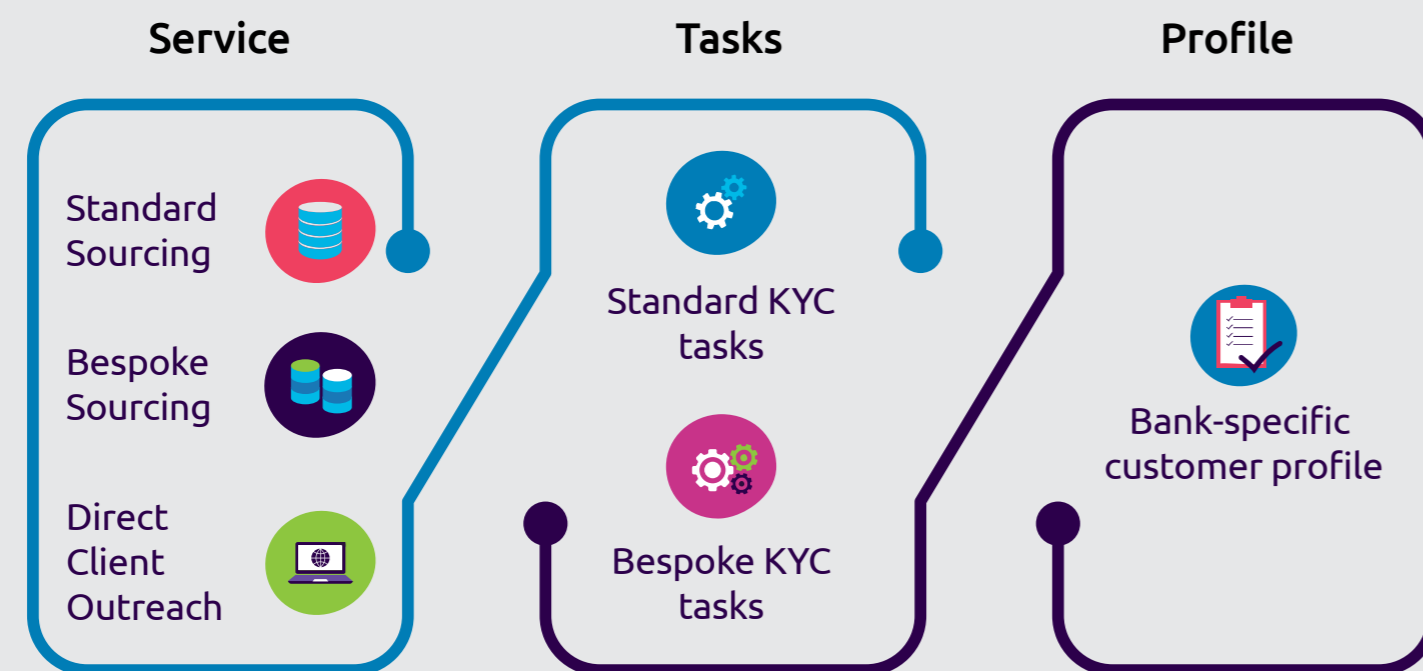


Advanced data-sourcing capabilities: Data collection should rely on the best technologies to foster automated sourcing, streamline data aggregation and refine quality assessments. The solution should also offer ways to segregate proprietary data from public one. Sourcing preferences of any bank or location should be available.



Automated end-to-end KYC tasks offering: As mentioned, the next-generation 'KYC-as-a-Service' solution should be able to propose a large scale of KYC tasks from data collection to final risk assessments. Those tasks would be available in a catalogue of available services and would foster automation and straight-through-processing at maximum, thanks to a combination of the latest technologies. Users would be able to mutualize or share service catalogue elements, processes and/or data.

Figure 14: A service catalogue offering to provide Bank-tailored KYC profiles



Tamper proof audit trail and proof of process: An end-to-end audit trail should be provided in real time to banks to enable constant monitoring of process successfulness, but also to demonstrate how the process was executed, by whom, when and supported by which dataset. To be compelling, and constitute an absolute proof of process, this audit trail needs to be tamper-proof.



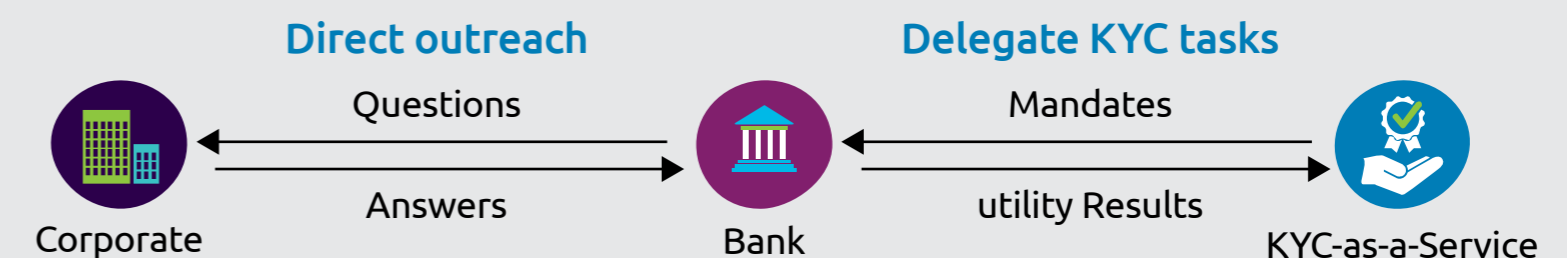
Activity Monitoring: The performance of the solution should be measured through KPIs, tracking agreed indicators (e.g. operational efficiencies, levels of mutualization, improved customer experience, cost reduction, quality, time to market, SLAs etc.). The solution should propose a way to extract and exploit those KPIs (dashboards, etc.) to provide all the necessary elements for the follow up of service levels, invoicing etc.

Benefits of a KYC-as-a-Service solution

Finally, by bringing together all the mentioned features, coupled with best-in-class technologies, the KYC-as-a-Service solution should bring customer experience to a higher level, thanks to automation and mutualization, while delivering the following value proportion to banks:

- Providing Financial institutions with **advanced Customer profiles updated on-demand**
- Banks and their subsidiaries can decide the way they want to handle customer outreach
- Enabling the delegation of a comprehensive part of the bank's KYC tasks
- Can propose to banks' **shared services in a standard catalogue of services**
- Enabling banks or banks' entities to opt-in for mutualized and/or bespoke levels of KYC services, including from a solution standpoint.
- **End-to-end and tamper-proof audit trail** on the data shared and the process managed (proof of process)

Figure 15: Next-Gen KYC-as-a-Service target operating model



Within such a KYC-as-a-Service solution, the benefits for financial institutions would be many:



Customer experience will benefit from accelerated time-to-business, thanks to faster onboarding processes. Also, by letting Banks or their entities keep direct and private access to their corporate customers, both customers and front offices will not suffer from any disintermediation.



Compliance will be improved thanks to their capability to delegate partially or totally the end-to-end KYC value chain to an entity providing best-in-class services. Banks will be able to propose or benefit from mutualized services, shared services and bespoke services (i.e.: Remediation). The tamper-proof audit-trail feature will let them keep the control on the KYC processes they have delegated to the operating entity, by ultimately owning the proof of process.



Operations will also benefit from up-to-date automation capabilities and the flexibility of relying on a service catalogue. In the end, financial institutions could rely on the KYC-as-a-Service solution to decommission or reallocate a large part of their current KYC processes and but also to help with their remediation projects. They will benefit from the latest technologies, thanks to a simplified FI integration with the use of internal APIs and Bank-specific policies.



Conclusion

KYC and CDD processes remain very costly processes that force banks to operate redundant tasks that affect overall customer experience.

The development of digitization and automation has transformed the way data collection and maintenance processes are handled, enabling better data quality, straight-through processing and ultimately better compliance and improved customer interactions.

Moreover, as KYC/CDD compliance systems work like a connected network of partners, the development of collaborative infrastructures is slowly opening the horizon of compliance to more inclusive systems and models, where each stakeholder is connected to each other. The benefits created by this interconnectivity are accelerated time to business and improved compliance.

In such environments, technologies like API, Intelligent automation, Artificial Intelligence and Distributed Ledger Technology provide new efficiencies, better data quality, improved controls and increased data lineage.

The confidence brought in by those technologies to the processed data enables new models of services, where data can appropriately be handled and processed by mandated parties with very limited risks of alteration or mishandling. This leads finally to the emergence of “KYC-as-a-Service” solutions, providing financial institutions a way to delegate their KYC operations to defined locations or actors, and encouraging collaboration by enabling mutualized and shared services. Those solutions, designed to allow significant costs reduction and improved customer experience, would enable more flexibility for daily KYC/CDD operations and high-tailored service capabilities.

The path to “KYC-as-a-Service” solutions can start by a maturity assessment relying on five pillars:

- Organization assessment
- Data assessment
- Process assessment
- Technology assessment
- Cost assessment

The conjunction of the maturity calculated for each of those pillars should give a clear picture of where the institution lies in its KYC/CDD transformation journey and the potential outcomes it could gain from bringing it one or several steps forward.

It should also give a clear view on the specific areas of improvement for the institution and where implementing new solutions can immediately provide measurable added value.

Wherever banks stand on their KYC transformation journey, deploying CLM tools and connecting to external data providers, we believe that implementing a KYC-as-a-Service solution that fits their organizational structure has the power to dramatically improve KYC operations, while reducing costs and improving customer experience.

In an increasingly complex, competitive, and challenging environment, banks need to ask and assess where they would like to be in the next five to ten years with the KYC functions. It’s no longer only a compliance requirement. The financial institutions which are able to understand and embrace change quickly and effectively will have a competitive advantage.





Authors



Preeti Malik

Global Head, Risk and Financial Crime Compliance
Insights and Data, Capgemini Financial Services

preeti.malik@capgemini.com

+1 416-770-8151

 [Connect with Preeti on LinkedIn](#)



Mathias Ros

Blockchain & B2B Platforms
KYC/AML Business Domain Expert
Capgemini Business Services

mathias.ros@capgemini.com

+33 7 60 65 08 66

 [Connect with Mathias on LinkedIn](#)

Acknowledgements:



Damien De Chillaz

Head of Blockchain & B2B Platforms
Capgemini Business Services

damien.de-chillaz@capgemini.com

+33 6 64 85 63 07

 [Connect with Damien on LinkedIn](#)



David SITBON

Head of Financial Services Continental Europe
Insights & Data Global Business Line

david.sitbon@capgemini.com

+33 7 61 47 71 81

 [Connect with David SITBON on LinkedIn](#)



Jean-Charles CROIGER

Director, Financial Services Compliance
Capgemini Invent

jean-charles.croiger@capgemini.com

+33 6 60 66 32 14

 [Connect with Jean-Charles on LinkedIn](#)

To learn more on our KYC and Financial Crime Management services, contact us at financialservices@capgemini.com



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.

The information contained in this document is proprietary. ©2020 Capgemini. All rights reserved. Rightshore® is a trademark belonging to Capgemini.