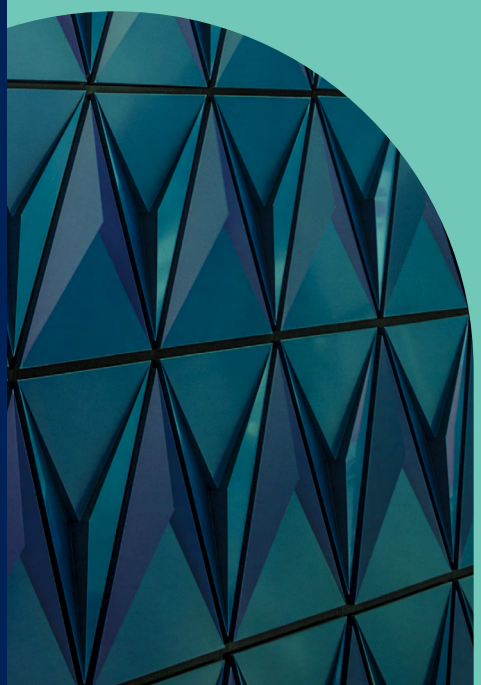
Know Your Customer

White Paper

The Future of KYC Compliance

How to embrace digital KYC to overcome the challenges of today and seize the opportunities of tomorrow.



knowyourcustomer.com

Index

Introduction

The world of KYC compliance is at a turning point.

In 2020, a series of **trends** that had been **in the making for years**, combined with the unprecedented circumstances brought about by the coronavirus pandemic, culminated in structural changes in the overall KYC compliance function at financial institutions around the world. This colossal shift is bound to shape the face of the sector for at least the next decade. Those financial institutions able to embrace change quickly and effectively will gain a competitive advantage that other contenders will struggle to match.

What you will read in this white paper

In this white paper we set the task to analyse the following:

- **The evolution of KYC compliance** – What do most compliance departments at financial institutions look like today? What has historically been the role of regulators in driving digital transformation and technology adoption? What are customers' expectations in shaping the change?

- **What the KYC compliance of the future looks like** – What are the key characteristics of the next phase of KYC compliance? What are some of the weaknesses of the traditional approach that the global COVID-19 pandemic brought to the fore?

- **The elements of a successful digital KYC implementation** – What elements should financial institutions consider before embarking on a digital transformation journey of their KYC function? What steps can teams take to ensure the success of their RegTech implementation?

- **How digital KYC providers can help** – What are the benefits of partnering with an experienced third-party provider to implement digital KYC solutions? What are some of the pitfalls that can be avoided by relying on external vendors?

Chapter 1: The evolution of KYC compliance

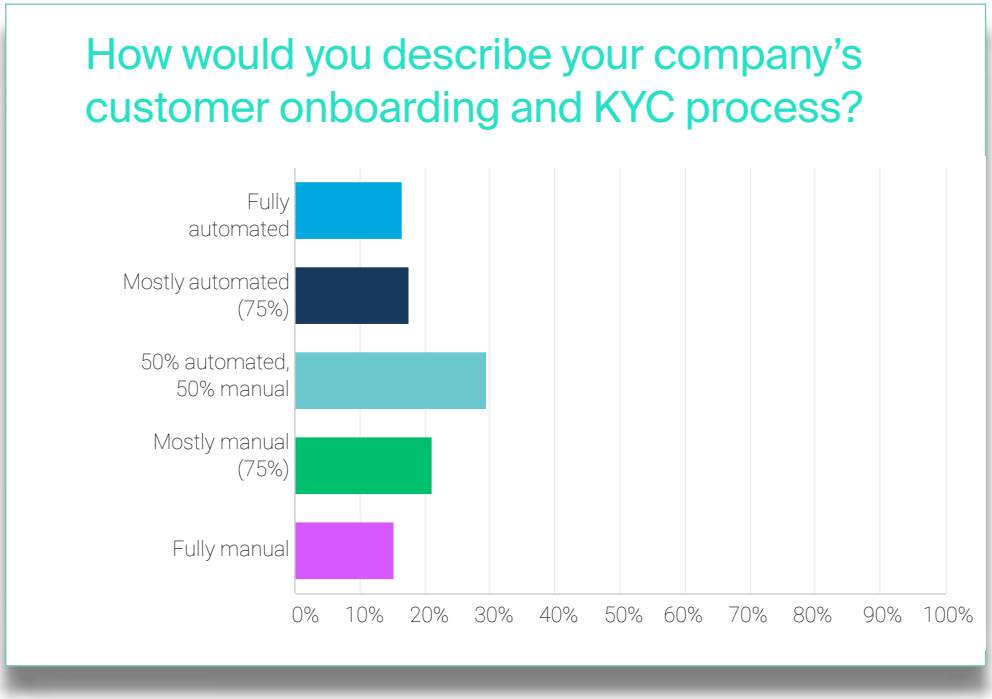
The current status of KYC compliance is one characterised by crucial transitions in all its aspects.

Firstly, this transition is part of the **overall digital transformation in financial services** trend that has been dominating the industry for quite some time. According to a study on the *State of Digital Transformation in Financial Services* published by Forrester in February 2020[1], 40% of surveyed FS firms were undergoing a digital transformation process before the COVID-19 crisis. The same study reveals that 19% of surveyed firms were still "investigating how to execute digital transformation" but had not yet begun.

Historically, the compliance department has been one of the last functions within financial services firms to embrace digital transformation.

A **general reluctance to steer away from established processes** caused the compliance function to remain an extremely manual and paper-based process. Even when it involves a digital element, this is often through a traditional system within an on-premise IT infrastructure that can only be accessed from the machines at the office.

Focusing on KYC compliance, a study by Know Your Customer conducted at the beginning of 2020 (*see graphic below*) revealed that **37% of surveyed compliance professionals** still rely on a "**fully manual**" or "**mostly manual"** customer onboarding and KYC process, while 29% of respondents describe their KYC procedures as "50% automated and 50% manual".



Transition and change also characterise the **overall regulatory approach to KYC compliance** in recent times. Financial regulators have started to replace diffidence with encouragement regarding technology adoption and digital transformation for AML/KYC processes. This shift, which had already started, was massively accelerated by the coronavirus pandemic.

For instance, during the inaugural AML/CFT RegTech Forum in November 2019, the **Hong Kong Monetary Authority** encouraged Hong Kong's banks to "consider, test and implement" RegTech solutions to drive innovation and stronger compliance across the sector.

During the inaugural AML/CFT RegTech Forum in November 2019, the Hong Kong Monetary Authority encouraged Hong Kong's banks to "consider, test and implement" RegTech solutions to drive innovation and stronger compliance across the sector.

Then in April 2020, following the official recommendations to promote digital onboarding solutions during the pandemic issued by the **Financial Action Task Force (FATF)**[2], the Hong Kong regulator reiterated the importance of remote client on-boarding and simplified due diligence for financial institutions. An official letter[3] by the Executive Director of the Hong Kong Monetary Authority (HKMA) stated that more than **10 Hong Kong retail banks** had already introduced remote account opening services since the beginning of the pandemic, while many more financial institutions were actively considering or testing similar approaches.

Moreover, a report on "COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses"[4] published by the Financial Action Task Force (FATF) in May 2020 highlighted that a number of **national regulators** have begun to encourage "the use of responsible digital identity and other responsible innovative solutions for identifying customers at onboarding and while conducting transactions".

This follows the FATF's own Digital ID Guidance[5] – released in March 2020 – which states that "non-face-to-face onboarding and transactions conducted using trustworthy digital ID are not necessarily high-risk and can be standard or even lower-risk".

Following the encouraging signals in certain markets, financial institutions have now started picking up the pace of digital change. However, in some industry segments, a number of challenges remain, including:

- A **general reticence** to replace **established manual processes** with new digital-first solutions;
- A traditional **delay** from IT departments in embracing technology trends that would accelerate the change, such as cloud computing solutions and "BYOD" (Bring Your Own Device) practices to facilitate **remote and flexible working;**
- **Limited opportunities to think strategically** about the role of compliance in shaping business processes, finding solutions that are efficient, fully compliant, and easily scalable to grow across international markets despite growing operational costs and regulatory requirements;

- A **lack of clarity from some regulators** on what constitutes a compliant process in the digital vs paper-based environment.

As daunting as these challenges maight have seemed historically, the risk of doing nothing has now become too great to ignore. Customers' **expectations of smooth and digital experiences** are becoming more and more engrained every day, fostered by the convenience and ease of use that new FinTech players are able to provide.

We don't know yet what the long-term impact of the coronavirus pandemic will be on FinTech 'unicorns'. However, customers who have experienced the type of digital KYC journey that companies like Revolut or N26 are able to provide will not go back to certified paper copies of documents or multiple trips to their bank branch when they need to open a bank account or access other financial products.

So, if financial institutions want to prepare their back-end as well as client-facing operations for the challenges of the next decade, the KYC compliance function is a great place to start.

Chapter 2: What the KYC compliance of the future looks like

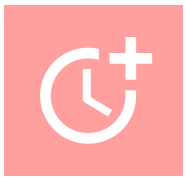
According to a Deloitte report on "Digital transformation for the risk and compliance functions"[6], one of the constant obstacles to compliance innovation has been the continued view of **compliance** and internal audit organisations as **"cost centres"** rather than "strategic business partners". However, as financial institutions and regulated organisations review their internal structures with the objective to equip their businesses for the challenges of the future, it is essential that they avoid falling into this trap.

The trends that we have explored in the previous chapter – accelerated by the COVID-19 pandemic in 2020 and 2021 – are changing KYC compliance as we know it. The traditional paper-based, manual, and sporadic process will be replaced by a KYC compliance approach that is:

Digital First

Customer-centric

Powered by scalable automation



On-going and on-demand

Driven by the principle of "compliance by design"

2.1 Digital-first

Before the COVID-19 pandemic, only around 5% of the UK workforce[7] and around 7% of the US workforce[8] used to regularly work form home. Then, in a matter of weeks, government-imposed lockdowns forced businesses in all sectors to embrace remote working.

Everywhere from New York to Seoul, corporate IT teams had to let go of their traditional mistrust of **BYOD (bring your own device) practices** and implement procedures enabling staff members to continue their work from home on their personal computers, tablets or mobile phones. Already in mid-March 2020, a Harvard Business Review survey[9] revealed that nearly 60% of employers indicated that they had increased employees' flexibility for remote work (46%) or were planning to (13%). Almost overnight, the office-based paradigm was replaced by the **remote access standard**.

Due to the predominantly intangible nature of their products, financial institutions are among the sectors that can clearly maintain a remote working approach even after the storm has passed. A full digitisation of the compliance function will help businesses enable their compliance officers to work from home. More specifically, **migrating all compliance's internal systems** to **cloud-based solutions** will enable financial institutions to easily introduce remote access to all their relevant workforce, without the need to massively increase on-premises server capabilities or allocate extended budgets from the beginning.

A full digitisation of the compliance function will help businesses enable their compliance officers to work from home.

Even traditional organisations whose internal policies do not allow for a cloud-first approach are beginning to experience the benefits of a hybrid approach to data security. In this model, core software functionalities live in the cloud (where they can be continuously upgraded and improved) while sensitive customer data is kept on premises.

2.2 Customer-centric

Moving back-office functions to the cloud and enabling compliance teams to work remotely are key steps towards the KYC compliance function of the future. However, digitisation should not be intended as a purely "behind the scenes" exercise.

Today's customers expect 100% mobile solutions and effortless client service delivered digitally and via their device of choice from the very beginning of their business relationship.

Financial institutions and regulated organisations will also embark on a journey to **transform their front end interactions** with prospective and existing customers. This is not only a matter of internal efficiency, but it is increasingly becoming a business development argument as well.

In fact, today's customers expect 100% mobile solutions and effortless client service delivered digitally and via their device of choice from the very beginning

of their business relationship, including in financial services. In this space, traditional financial institutions may have a lot to learn from **up and coming Fintechs**. A lack of resources has often pushed new players in the financial services space to experiment with new and more efficient ways of interacting with customers. Some of these techniques are now becoming the industry standard and customers have begun to expect them from their traditional banks as well.

Research from Gartner[10] predicts a 400% increase in the use of AI to handle customer service interactions in the 2017- 2021 period. What might have been introduced as a necessary solution to assist customers during onboarding without having to rely on staff's intervention may soon become a requirement that customers expect from all of their FS vendors.

2.3 Powered by scalable automation

Automation's strength is its ability to **quickly and consistently scale** the efforts needed to enforce **compliance procedures** across an organisation and geographies in a way that limits frictions in the user journey. This is a fundamental ingredient for commercial and operational success in the era of growing financial regulations and more demanding customer expectations.

However, a general uncertainty regarding the ability of automated processes to **catch nuances and identify red flags** – maybe based on past experiences with early automated processes – is still present in the industry. The last decade has seen incredible progress in the application of **artificial intelligence** and **machine learning** to better understand – and learn from – available sets of data. Additionally, the secret to successfully embracing compliance automation lies in what can be called **intelligent automation**. The intrinsic value of automation is extremely visible when it replaces manual and repetitive tasks, freeing up time for compliance teams to review limit or suspicious cases that automation on its own would not be able to work through.

The areas where an automation-driven approach to compliance is particularly beneficial include:

1. **Security and customisation** during document collection, only requesting necessary documents and removing the need to send back and forth emails with attachments (all documents are automatically and securely uploaded to the relevant case);

2. **Ability to scale volumes of activity** through cloud technology or commercially expand into new markets by easily adapting customer workflows to reflect current requirements across jurisdictions;

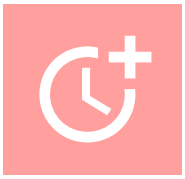
3. **Reliable** AI-powered checks for **authentication of international ID documents**;

4. **Extraction via Optical Character Recognition** of key information from incorporation documents for corporate clients, as well as automated transliteration from multiple character sets and languages your team might not be familiar with;

5. **Automated audit trails** to record all actions and checks performed on any given customers;

6. **Tiered access** to documents and functionalities based on team members' roles and responsibilities.

2.4 On-going and on-demand



Most AML regulations around the world require financial institutions and regulated organisations to **know their customers' position at all times**.

However, implementing real on-going checks using a traditional and manual approach is not only hard, but also extremely inefficient. To have a truly satisfactory coverage, compliance teams would have to manually perform all their checks multiple times per month, heightening the **risk of human error**.

Implementing real on-going checks using a traditional and manual approach is not only hard, but also extremely inefficient.

However, by implementing technology that runs **AML checks automatically in the background** and instantly flags any changes in customers' circumstances in real time, compliance teams can meet the regulators' requests for on-going compliance without having to allocate additional human resources to the task. Platforms that also include a **Live Monitoring** feature for **all Proof of Identity documents** can identify upcoming expiry dates and alert customers to upload updated documentation well in advance of the deadline through a system of automated reminders.

The ability to promptly perform additional **recertification or AML checks on demand** or generate customised **internal and external reports** when the compliance team needs them is another one of the many advantages of a technology-first approach to KYC compliance.

2.5 Driven by the principle of "compliance by design"

To this day, many compliance teams at financial institutions are still working with a variety of **disconnected technologies** and **complex manual processes** that make true collaboration and innovation extremely difficult.

Rather than embarking on digital transformation journeys in unchartered waters, risk-averse businesses might prefer to outsource some or most of their compliance workload to large teams of external consultants. However, the solution that seems prudent at the time may reveal itself as the more short-sighted in the long run.

On-going regulatory evolution is a key requirement to effectively combat money laundering and financing of terrorism on a global scale. To keep up with new and stricter requirements as they are introduced, technology is of the essence.

By implementing flexible technologies that can be seamlessly adapted to reflect new requirements and workflows as they are introduced, financial institutions can limit their exposure to AML-related fines.

By implementing **flexible technologies** that can be seamlessly adapted to reflect new requirements and workflows as they are introduced, financial institutions can embrace the concept of "compliance by design" and limit their exposure to AML-related fines. The strategic use of technology empowers compliance teams to **embed governance and control into business practices** in a way that no compliance training – however well planned and executed – could ever achieve.

After the implementation phase, efficiency gains can be substantial.

According to a research report by Globalscape and Ponemon Institute[11], companies that enabled compliance technology **save** an average of **$1.45 million per year** in compliance costs.

Interestingly, regulators have an important role to play in driving this change of perspective. The existing trends towards stricter and more frequently updated anti-money laundering regulation will continue to develop in the coming years. By **encouraging RegTech adoption** among their regulated entities, regulators are better positioned to accelerate the introduction of more stringent KYC/AML requirements, which can only be met through an intelligent use of automation.

Chapter 3: The elements of a successful digital KYC implementation

A digitisation project is an extremely unique opportunity to introduce solutions and procedures that will shape the way staff work on a day-to-day basis for a long time. Such a perspective – however daunting – can help fully appreciate why all digital transformation journeys – however complex, however extended – should embrace the concept of *agility*.

This term – which in the software development community describes a very specific way of writing code and building products – can be applied to many more aspects of digital transformation in financial services' compliance.

The term agility can be applied to many more aspects of digital transformation in financial services' compliance.

In the space of digital KYC, it translates as follows:

1. **Agile planning**: plan for change in all its aspects by setting out a roadmap that you can adjust as you learn more about your customers' preferences, your teams' needs or the regulatory requirements of new jurisdictions you want to grow your business in; make sure different departments get involved by bringing to the table their own expertise in regulatory compliance, risk, UX/UI, Customer Support, or IT;

2. **Agile technology**: whether building in-house software or partnering with a third-party, choose flexible digital solutions that can be configured based on your specific needs and internal processes and changed over time;

3. **Agile regulatory set-up**: make sure that your new systems and procedures are fully compliant with the regulations of today, but can also be adapted to the regulations of tomorrow, or the regulations of another jurisdiction your business will be growing in;

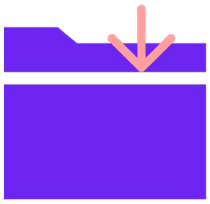
4. **Agile scope**: Rome wasn't built in a day, and full digital transformation never happened overnight; start from a pressing problem while keeping in mind the big picture, which will help you achieve tangible goals on the way to long-lasting change.

Introducing a "**digital work space**" that empowers compliance teams to collaborate in a similar way to what they would be doing at the office is the first step of any true digitisation journey.

The quickest way to achieve this is for financial institutions to implement **cloud-based document management system** that securely stores all relevant information and collected files about prospective customers in one centralised location. This integrated system should not be a Drop Box-like filing cabinet that anyone can open. It should include a workflow system so that team members can exchange information,

comment on progress and assign specific tasks to one another to complete all required KYC & AML checks. In the new remote working context, the advantages of cloud-computing are particularly evident. Not only staff can access cloud solutions from their own devices wherever they are in the world, but these platforms are also able to scale along with the organisation's needs for data storage and user permissions.

Then, teams should move on to analyse the key pillars of the KYC process in its purest essence and identify how each one of these could be digitised. The **five pillars** of the KYC process can be summorised as follows:



DOCUMENT COLLECTION

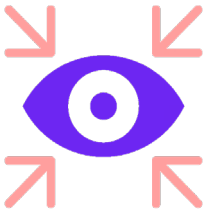
Collect required documents from prospective customers

DATA ASSESSMENT

Investigate and verify data & documentation provided by customers

CASE MANAGEMENT & WORKFLOW

Translate compliance policies into step-by-step processes

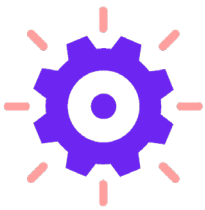


ON-GOING MONITORING

Continous checks to monitor and flag customers' change in situation

REPORTING & INTELLIGENCE

Analyse data about internal activity to create internal, external & regulatory reports



The **level of digitisation** that a company decides to embrace may depend on their available resources at the time of planning. However, opting for a **"step-by-step" approach** – where action A represents the solid base on which Action B and Action C can be built – may help financial institutions save considerable amounts of time, effort and budget in the medium to long term.

The table below provides a few example of this tiered approach to the digitisation of the KYC compliance function.

	Document Collection	Data Extraction and Assessment	On-going Monitoring	Reporting & Analysis
Action A	Standard mobile app or secure web portal to limit cybersecurity exposures Manual access by staff to online registries to retrieve incorporation documents	ID verification solution to flag fraudulent ID documents Manual transposition of company's details from official documents to a centralised digital KYC repository Ad hoc UBO charts based on inputted information by staff	Checks prospective customers with standard AML provider for PEP, sanctions, adverse media based on a standard check	Standardised digital reports securely stored in the company's cloud
Action B	Branded mobile up or secure web portal for a seamless customer experience Automated retrieval	Automated extraction of individual customers' details from ID documents and official registry documents Identification of UBO and instant unravelling of company structure charts across jurisdictions	Integrated AML review of all new and existing customers in the system	Automated KYC reports for different client types for audit purposes
Action C	Full integration with digital due diligence platform, CRM system and company website/ mobile app through Rest APIs AI-driven chatbot to guide the prospective customer through the document collection step	Automated requests for additional information based on non-satisfactory facial comparison and liveness detection checks Automated requests to upload missing information from corporate customers before triggering compliance teams' involvement	Additional expired Proof of Identity alerts in advance, preventing out of date information being stored in the system	Fully automated Business Intelligence tool for team's activity review and on-demand customised reports (internal, external)

Chapter 4: How digital KYC providers can help

Rather than building expensive in-house systems for digital KYC from scratch, an ever-growing number of financial institutions decide to **partner with third-party RegTech providers** to better ensure the success of their digitisation journey.

These specialist solutions – when properly implemented – empower compliance teams to securely collect documents from their remote clients via multiple digital tools and instantly extract and verify the information provided through Optical Character Recognition and Artificial Intelligence.

Compliance officers can then access and review all the collected information within one centralised online platform, automatically perform on-going AML monitoring and instantly receive alerts of any changes in the client's situation or associated risk, irrespective of the location of both the client and the compliance officer.

Although no two companies are 100% alike, relying on third-party vendors may help financial institutions avoid a number of missteps and **anticipate potential road blocks**.

When it comes to digital KYC projects, all the learnings accumulated by third-party software providers in the course of months and years can guide customer teams through each step of the implementation process and help them **achieve success within the required timeframe**.

When it comes to digital KYC projects, all the learnings accumulated by third-party software providers can help financial institutions achieve success within the required timeframe.

As the number of available options grows, compliance teams should thoroughly investigate which vendors offer the solutions that are best-suited to address their specific challenges, while also providing the following:

- **Regulatory compliance** – Compliance expertise and deep knowledge of local financial regulations should be built into the system's workflows to accelerate implementation.

- **Remote access** – As remote work becomes the norm rather than the exception, cloud-based solutions that can be securely accessed from employees' homes are becoming a must of digital KYC. If it lives in the cloud, a centralised platform can become a golden source of information for all team members, where data is updated and sourced in real time and all actions and decisions are automatically tracked in an immutable audit trail.

- **Architecture scalability** – This is key to adapt to new regulatory requirements as they are introduced, as the customer base sensibly increases within new or existing markets or as the team grows across jurisdictions around the world.

- **Seamless customer experiences** – As consumers' expectations evolve, so should the customer onboarding experience that organisations are able to deliver. Similarly, any digital KYC solution should be configurable to allow for multiple digital journeys based on different types of clients.

- **Ability to integrate multiple legacy systems** – Harmonising multiple systems through a dynamic solution is fundamental to ensure the success of any digital compliance strategy. In this sense, a vendor that not only offers a full range of APIs, but also provides comprehensive documentation to make life easier for your IT team is key.

Conclusions

In conclusion, 2020 represented a key turning point in the evolution of KYC compliance.

Digital transformation trends that had been long in the making were drastically accelerated by the unprecedented global situation determined by the COVID-19 pandemic. With offices being inaccessible, remote working and cloud-based solutions became the primary way to avoid interruptions in the provision of financial services. For the KYC compliance function, in many cases that meant replacing paper-based, highly manual and extremely inefficient procedures with digital-first, automated and customer-centric processes almost overnight.

At the same time, we have witnessed a shift in regulators' approach to establishing and enforcing their AML requirements. Guided by the FATF, regulators across Europe and Asia have started to embrace digital technology for remote onboarding more decisively than ever before, accelerating the pace of RegTech adoption even further.

In this regard, while building digital solutions in-house may seem like the appropriate option in certain cases, **partnering with specialised third-party providers** can help financial institutions drastically accelerate the digital transformation of the KYC compliance function. Powered by today's innovative technology, compliance teams can quickly and effectively achieve an **intelligent, scalable and compliant digitisation** of all the key pillars of their KYC compliance process, reaching a level of accuracy and reliability even higher than traditional "in person" checks for the remote onboarding of all types of clients.

On the **individual side**, the width and depth of available ID verification technology now includes AI-driven ID document checks, video verification, liveness detection, automated facial comparison, geolocationing, and on-going AML screening options that can help compliance teams add extra layers of security to their digital onboarding journeys.

From the **business verification and KYB** point of view, state-of-the-art digital solutions offer seamless connections to company registries around the world, automated retrieval of mandatory documents based on local regulatory requirements, automated transliteration from a variety of character sets, transcription of key information through Optical Character Recognition, instant unravelling of UBO charts and secure outreach tool for shareholder information.

As explored in detail throughout this white paper, the new normal determined by the COVID-19 pandemic together with a renewed attitude of regulators towards RegTech and the possibilities offered by solution providers on the market are contributing to the creation of a new KYC compliance paradigm.

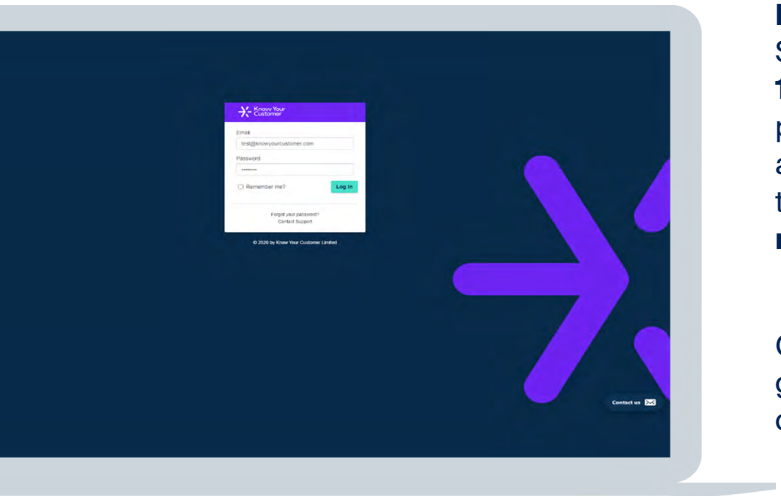
The new normal determined by the COVID-19 pandemic together with a renewed attitude of regulators towards RegTech and the possibilities offered by solution providers on the market are contributing to the creation of a new KYC compliance paradigm.

Instead of the traditional paper-based, manual, and sporadic process, the new approach to KYC compliance is **digital-first**, **customer-centric**, **powered by scalable automation**, **on-going and on-demand**, and **driven by the principle of "compliance by design"**.

By embracing the new paradigm early, financial institutions can leap ahead of the competition, providing the type of onboarding experience regulators demand and customers expect.

If you are looking to equip your compliance team against the challenges of today and tomorrow and are ready to embark on a digital transformation journey to change your KYC process, we'd love to help. **At Know Your Customer**, we specialise in providing scalable, flexible and dynamic digital KYC solutions to financial institutions around the world.

About Know Your Customer



Established in 2015, Know Your Customer is a **global RegTech company** with offices in Hong Kong, Dublin, Singapore, and Shanghai. Our clients span across **11 sectors** – including banking, FinTech, insurance, payments, real estate, asset management, legal, among others – and **18 jurisdictions** and are using our technology to verify and **onboard customers from more than 180 countries**.

Our technology enables organisations to ensure on-going KYC/AML compliance while digitising their customer onboarding process end to end.

To discover more about our range of digital KYC solutions, visit knowyourcustomer.com or request a demo here.

Know Your Customer

info@knowyourcustomer.com
knowyourcustomer.com

Know Your Customer
@KYC_ltd

Endnotes

1 https://reprints.forrester.com/#/assets/2/234/RES159658/reports

2 http://www.fatf-gafi.org/publications/fatfgeneral/documents/statement-covid-19.html

3 https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-andcircular/2020/20200407e1.pdf

4 https://www.fatf-gafi.org/publications/fatfgeneral/documents/covid-19-ml-tf.html

5 http://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identityguidance.html

6 https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-digitaltransformation-for-the-risk-and-compliance-functions.pdf

7 https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/articles/coronavirusandhomeworkingintheuklabourmarket/2019

8 https://www.weforum.org/agenda/2020/03/working-from-home-coronavirus-workers-future-of-work/

9 https://hbr.org/2020/03/8-questions-employers-should-ask-about-coronavirus

10 https://www.gartner.com/smarterwithgartner/4-trends-gartner-hype-cycle-customer-service-customer-engagement/

11 http://dynamic.globalscape.com/files/Whitepaper-The-True-Cost-of-Compliance-with-Data-Protection-Regulations.pdf#page=17