Market Quadrants

KYC/AML Software Solutions, 2020

Market Update and Vendor Landscape

Chartis

Independent. Insightful. Actionable.

About Chartis

Chartis Research is the leading provider of research and analysis on the global market for risk technology. It is part of Infopro Digital, which owns market-leading brands such as Risk and WatersTechnology. Chartis' goal is to support enterprises as they drive business performance through improved risk management, corporate governance and compliance, and to help clients make informed technology and business decisions by providing in-depth analysis and actionable advice on virtually all aspects of risk technology. Areas of expertise include:

- Credit risk.
- Operational risk and governance, risk and compliance (GRC).
- Market risk.
- Asset and liability management (ALM) and liquidity risk.
- Energy and commodity trading risk.
- Financial crime including trader surveillance, anti-fraud and anti-money laundering.
- Cyber risk management.
- Insurance risk.
- Regulatory requirements including Basel 2 and 3, Dodd-Frank, MiFID II and Solvency II.

Chartis is solely focused on risk and compliance technology, which gives it a significant advantage over generic market analysts.

The firm has brought together a leading team of analysts and advisors from the risk management and financial services industries. This team has hands-on experience of implementing and developing risk management systems and programs for Fortune 500 companies and leading consulting houses.

Visit **www.chartis-research.com** for more information.

Join our global online community at **www.risktech-forum.com**.

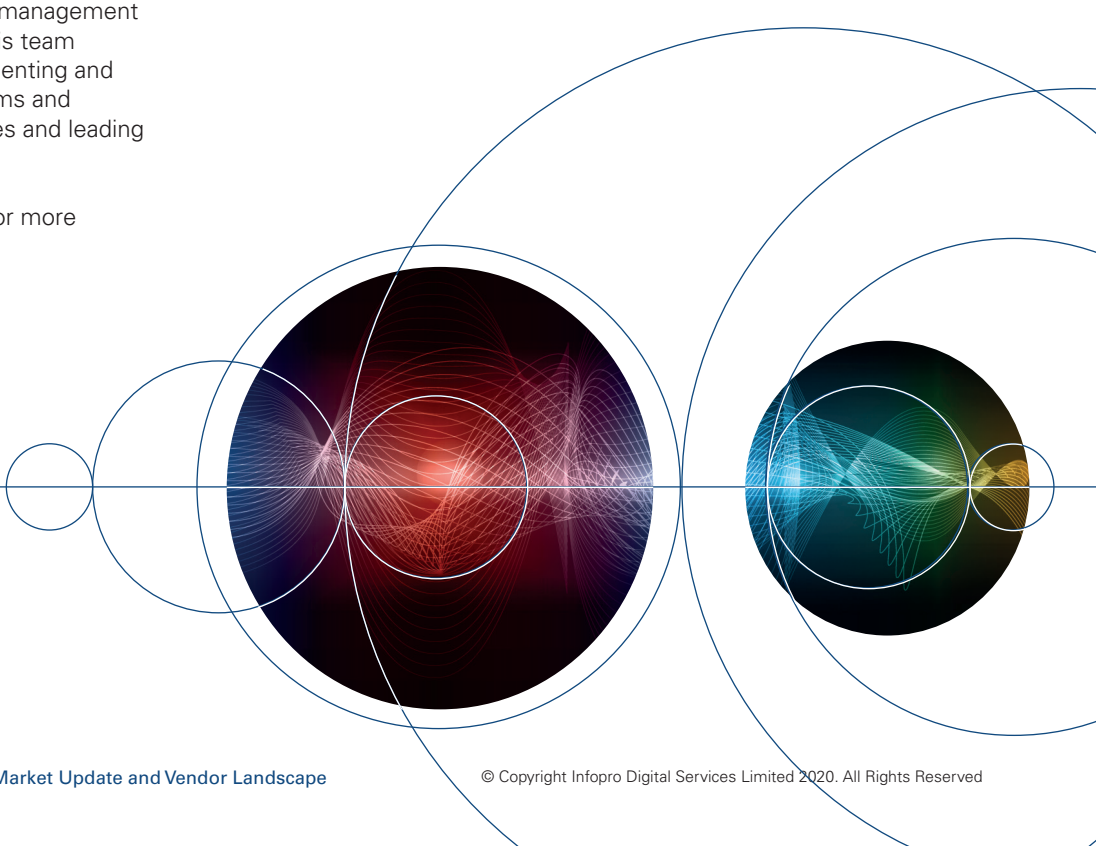


Table of contents

List of figures and tables

1. Executive summary

This report examines financial institutions' (FIs') evolving technology requirements for Know Your Customer (KYC)/anti-money laundering (AML) processes and systems. In FIs, many elements of KYC/AML requirements overlap to create a common compliance-orientated process. For this reason, we have chosen to address both solution types in a single report, to capture commonalities in their systems and processes, and in the vendor landscape.

In FIs, KYC/AML capabilities are bought primarily by the compliance side of the business, although a company's operational units have a significant role to play in KYC and customer onboarding. However, for the purposes of this report we consider the vendor landscape for both KYC and AML capabilities to be still largely compliance-driven, although within this context there is significant overlap between the KYC and AML areas. In addition, several AML vendors have migrated over to the KYC side of the market, complicating the picture. In light of all these factors, we consider a unified view to be the best approach for providing as comprehensive a view of the industry as possible.

Context: managing the human element

KYC/AML processes often include problems and challenges that are both repetitive and complex. Because the fines and risks associated with AML non-compliance remain high, FIs are investing heavily in KYC/AML solutions. However, the tenor and specificity of AML and KYC spend has changed – no longer are firms' compliance departments being given blank cheques to spend on technology solutions and staff. Instead, expenditure must be validated according to targeted business outcomes and return on investment. Automation and technology have a central role, although this is more about lowering the cost of human staff rather than entirely automating processes.

For many FIs, labor is a significant component of the cost of addressing financial crime. Because of the sheer volume of complex problems involved, and firms' near-zero risk appetite, created by a fear of sanctions and reputational damage, FIs have also been investing heavily in building large compliance teams to address their KYC/AML challenges. Compliance processes often cross multiple business lines and requirements, and managing this dynamic web has led to the operationalizing of KYC/AML – in other words, optimizing the human element, which drives many of the efficiency gains in KYC/AML processes. In this context, we will assess the important changes in the key elements of KYC/AML processes: outsourcing, data, analytics and workflow.

The COVID-19 effect

In our previous analysis we have considered the evolution of firms' digitization strategies, and have concluded that customer experience and onboarding times are both differentiators – faster and more efficient onboarding times lead to greater customer satisfaction and more onboarded customers – and significant sources of cost, because of labor and technology expenditure. Acting as a catalyst of change, the COVID-19 pandemic has accelerated these pre-existing trends. Many FIs have sped up their digitization projects, and their use of technology and large-scale workflow to manage the onboarding process. Increasingly, they are doing this without immediate recourse to their 'traditional solution' – hiring vast numbers of compliance and onboarding staff.

The pandemic has highlighted the need for flexible technology architectures, and the effectiveness of FIs' efforts to mitigate their risk exposure will depend ultimately on their willingness to develop new technology strategies and invest in systems and maintenance. Reducing false positives is a key issue, but benchmarking and testing it remains a huge challenge, particularly over longer timescales. We have thus seen a steady shift away from false-positive resolution as the primary metric in KYC/AML deployments, toward a range of measurements that address greater efficiency and return on investment (such as productivity metrics and number of onboarded clients).

More vendors, with specific capabilities

To accommodate FIs' evolving requirements, vendors have sharpened their focus on three key areas:

- Automation.

- Enhanced workflow capability.
- Enhanced data management.

Growing numbers of vendors – even those that have historically focused more on analytics and case management – now specialize in providing data-provision capabilities. Increasingly, the lines between data providers and software and analytics vendors are blurring. One of the main dynamics in the KYC landscape is the significant increase in the number of entrants in the space. Notably, vendors are addressing many different markets, so are competing less directly with each other. Firms have strengths in specific areas, such as retail, commercial and investment banking, wealth management, and broker-dealing.

In addition, they often provide separate parts of the KYC technology stack. As discussed in previous iterations of this research[1], few vendors provide a packaged end-to-end KYC solution; instead, many focus on providing specific capabilities such as case management, entity resolution or risk analytics. Data remains a key part of the KYC process, and the ability to build out entity relationships with proprietary data providers remains key to a durable market presence.

The number of vendors in the AML landscape is also growing, as more specialist firms enter this space and more competitors challenge the dominant players. For challengers, the key differentiating capabilities are typically transaction monitoring and case management. In general, winning vendors are increasingly providing solutions that offer scalability, usability and data security for KYC/AML processes.

This report uses Chartis' RiskTech Quadrant© to explain the structure of the market. The RiskTech Quadrant© uses a comprehensive methodology of in-depth independent research and a clear scoring system to explain which technology solutions meet an organization's needs. The RiskTech Quadrant© does not simply describe one technology solution as the best risk-management solution; rather, it has a sophisticated ranking methodology to explain which solutions would be best for buyers, depending on their implementation strategies.

This report covers the following providers of KYC/AML solutions: 3i Infotech, Accuity, AML Partners, Appway, Ayasdi, BAE Systems, BlackSwan Technologies, Clari5, ComplyAdvantage, Dow Jones, Featurespace, Fenergo, FICO, FinScan, Fiserv, GBG, Genpact, IBM, IHS Markit, iMeta, InfrasoftTech, Know Your Customer, KYC Global Technologies, LexisNexis Risk Solutions, Manipal Technologies, NICE Actimize, Oracle, PwC, Quantexa, SAS, ThetaRay.

We aim to provide as comprehensive a view of the vendor landscape as possible within the context of our research. Note, however, that not all vendors we approached provided adequate information for our analysis, and some declined to participate in this research[2].

[1] *See 'Financial Crime Risk Management Systems: Know Your Customer; Market Update and Vendor Landscape, 2019' and 'Financial Crime Risk Management Systems: AML and Watchlist Monitoring; Market Update and Vendor Landscape, 2019'.*
[2] *Note that references to companies in the text of this report do not constitute endorsements of their products or services by Chartis.*

2. Market update

Definitions and context

This report provides an overview of trends in financial crime compliance systems that include KYC and AML capabilities, which we combine into one report with a unified theme. This report builds on *Financial Crime Risk Management Systems: Know Your Customer; Market Update and Vendor Landscape, 2019* and *Financial Crime Risk Management Systems: AML and Watchlist Monitoring; Market Update and Vendor Landscape, 2019* as part of Chartis' financial crime risk-management series. In the context of this research:

- **AML** refers to all policies and procedures aimed at preventing money laundering, with a particular focus on name screening, case management and transaction monitoring.
- **KYC** is concerned with determining the accurate identity of a customer – a person or a company – and the risk to an FI of conducting business with that entity.

Many elements of KYC/AML requirements overlap to create a common compliance-orientated process (see Figure 1). (AML and compliance systems, for example, need KYC information in order to execute AML transaction-screening processes.) As such, we have chosen to address these within a common report format, to effectively capture the commonalities within the relevant processes and the vendor landscape.

FIs have invested heavily in technology to speed up KYC/AML processes

Fines associated with AML non-compliance remain high (see Appendix A for more information). But for many FIs, accurately deciding who they can and should do business with carries significant implications in terms of cost, time and resources. Compliance remains a significant challenge for FIs, because KYC/AML processes often include repetitive and complex problems. As a result, time-saving techniques (such as automation) can only be partially applied, especially because problems – which include entity resolution ('is entity X who they say they are?') and false positives ('is the analysis of risk associated with this entity correct?') – can change from simple to complex within a single workflow. This complexity is typically beyond the range of fully automated systems and requires human intervention.

But because money laundering plays a significant role in regulatory penalties and reputational damage, FIs are investing heavily in KYC/AML systems, and particularly in building large compliance teams and sophisticated technology solutions. To speed up decision making during the onboarding and ongoing monitoring of customers, for example, the data that FIs consult must be accurate, easily accessible, consistent, secure and regularly updated. FIs can employ machine learning (ML) tools to clean and process large volumes of data and reduce false positives.

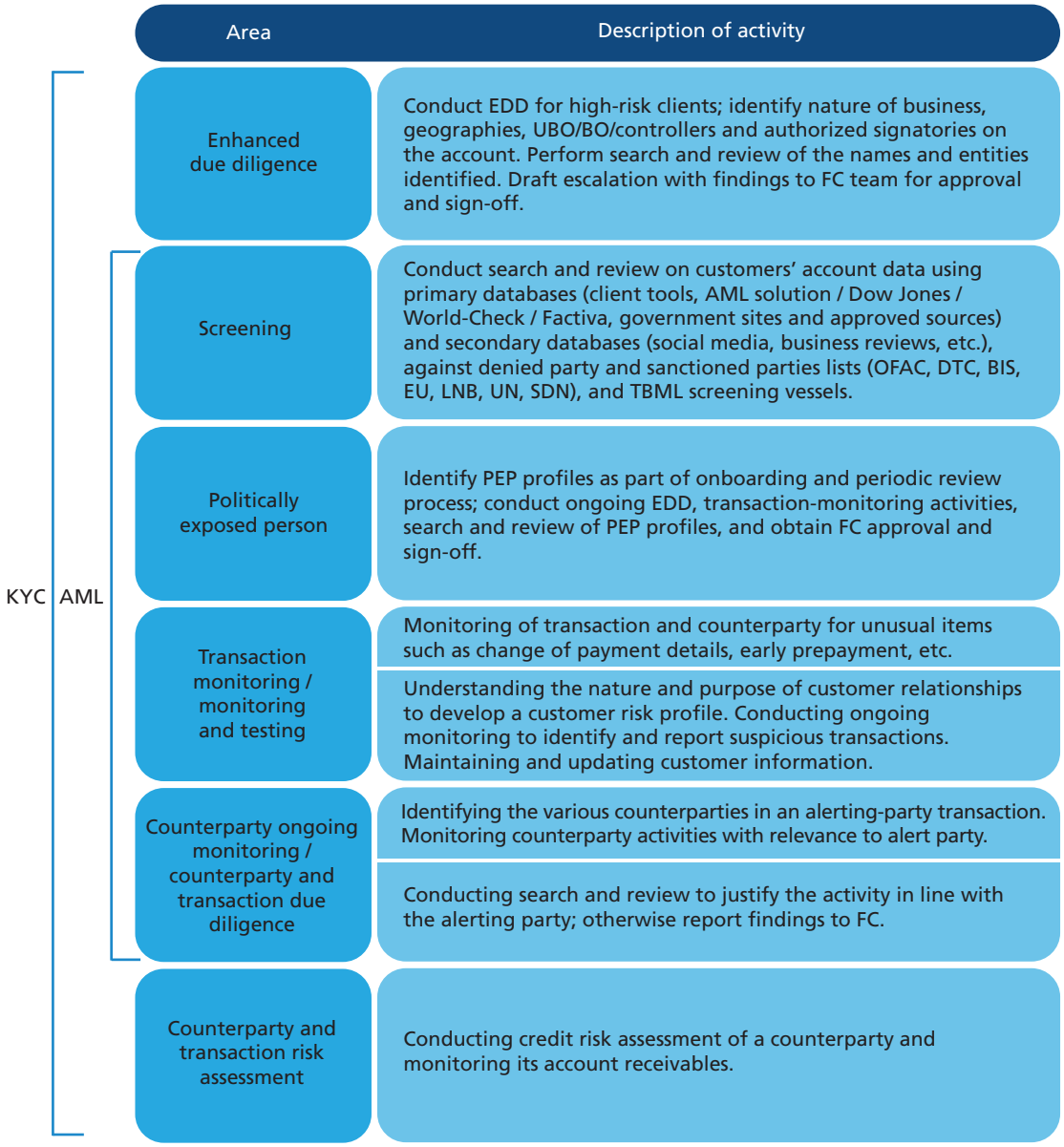
In fact, in the fight against financial crime, many regulators, including the Financial Conduct Authority (FCA) in the UK, have encouraged banks to leverage innovative technology[3] like ML-based techniques. But while there is encouragement for trying new solutions, FIs must be able to prove that they understand and can validate their models in line with the supervisory guidance of the Office of the Comptroller of the Currency (OCC) for model risk management (OCC 2011-12/SR11-7). They also need to prove that their advanced analytics are performant – model benchmarking should be used to prove that new techniques have significant advantages over traditional rules-based/stochastic systems and pre-existing rules libraries. The FCA has warned FIs that they will be fined if they adopt vendor-supplied systems that are not adequately tailored to match the size and complexity of their business. So while regulators are encouraging innovation, they need to be comfortable that ML systems are effective.

Humans are still required

ML and artificial intelligence (AI) cannot handle everything – the technology has its limits. Even advanced ML is a pattern-recognition exercise typically based on historical events. Its ability to handle end-to-end complex processes relies on good quality data and reliable training sets; true positives (i.e., correctly identified AML entities who have made it past the first layers of a sanctions screening process but are identified later) are often difficult to identify in the areas of KYC and AML. In addition, good technology requires adequate explanation and well-planned implementation. Finally, the sign-off for KYC/

[3] *See, for example,* **https://www.fca.org.uk/news/speeches/turning-technology-against-financial-crime**

Figure 1: Many elements of KYC and AML processes overlap



Source: Chartis Research

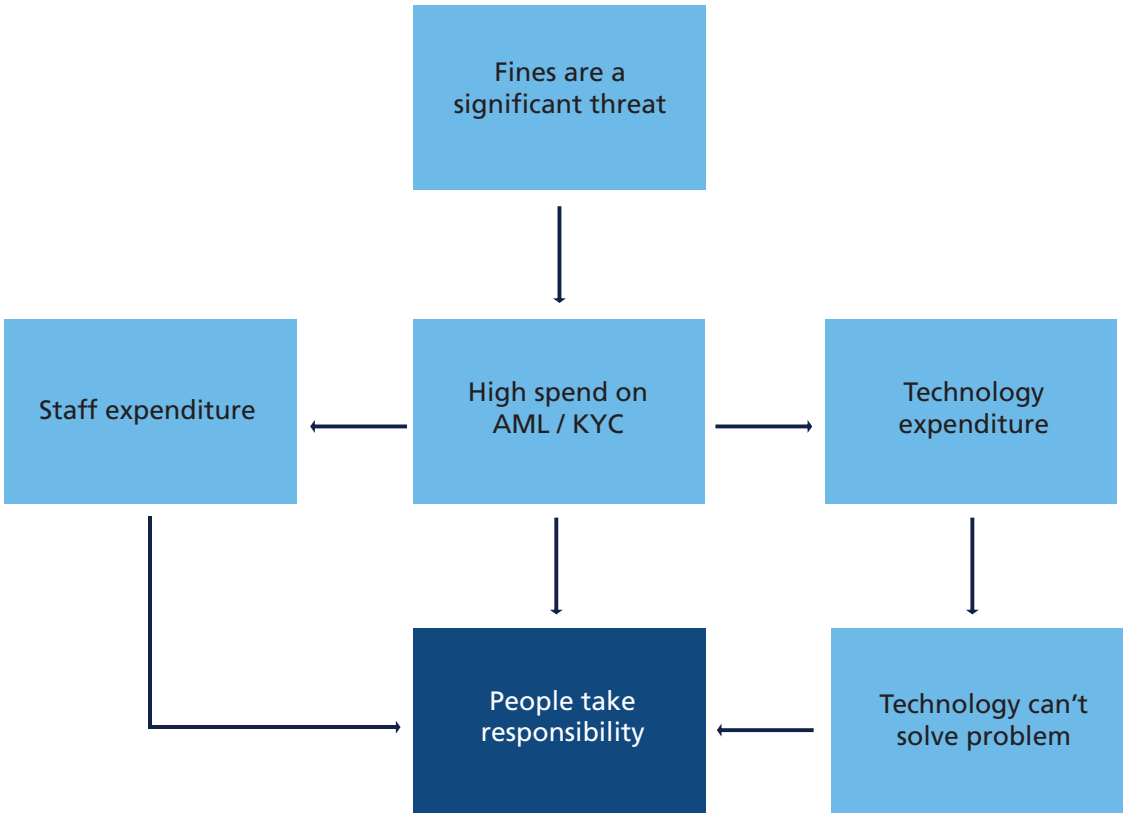
AML processes must always involve human responsibility (see Figure 2).

As such, KYC and AML are at heart human problems, and their solutions have always involved large numbers of humans (running counter to the idea that these systems can be fully automated). Because of the sheer volume of complex problems involved, combined with a near-zero risk appetite created by a fear of sanctions, FIs have also been investing heavily in building large compliance teams to address their KYC/AML challenges. The high cost of errors means that there must be accountability (a human sign-off, in other words), especially for more complicated decisions.

Consequently, for many FIs, labor is a significant component of the cost of dealing with financial crime. According to LexisNexis Risk Solutions' 2020 global cost of compliance study[4], the projected total cost of addressing financial crime compliance for FIs globally will be $180.9

[4] *See* **https://risk.lexisnexis.com/global/en/insights-resources/research/the-true-cost-of-aml-compliance-european-survey**

Figure 2: The human touch is vital in KYC/AML processes



Source: Chartis Research

billion. Labor is the single largest component in high compliance expenses: FIs spend 57% on average on labor costs, compared with 40% on technology and 3% on other factors. The average cost of compliance is significantly higher for medium-sized and large European firms, compared with those in other regions. The rising bills are the result of having to address more complex regulations (including data privacy restrictions such as Europe's General Data Protection Regulation [GDPR]), and increased scrutiny from regulators in this area. In addition, alongside more stringent regulations in Europe around ultimate beneficial owners (UBOs) – such as the 2016 FinCEN[5] Final Rule – banks are facing greater scrutiny in the wake of recent high-profile money laundering and sanctions-related scandals.

A focus on efficiency

In turn, FIs are assembling large teams, both in-house and through outsourcing, to demonstrate to regulators that they are working hard to maintain their compliance and catch AML violations. FIs often maintain large compliance teams because this makes sense from a cost-benefit perspective: should a sanctions violation occur, no FI wants to have been seen reducing their compliance staff. So, while we do not expect to see significant declines in the numbers of compliance staff FIs have, we do anticipate a heightened focus on efficiency and productivity.

Even as banks shed jobs in the wake of the COVID-19 pandemic, staffing and investment in compliance are likely to remain high, because of the significant risk of noncompliance. ING, for example, which was fined €775m by Dutch authorities in 2018 for a series of compliance failures, has since increased its spending on KYC and AML compliance systems[6] and voiced its support for the EU's proposals for a cross-border AML authority[7]. After a series of banking scandals in Europe, which exposed the patchy enforcement of AML directives across the bloc, the new enforcement body proposed by the European

[5] *Financial Crimes Enforcement Network.*
[6] **https://www.ing.com/About-us/Compliance/KYC-and-anti-money-laundering-measures.htm**
[7] **https://www.riskscreen.com/kyc360/news/ing-voices-support-for-creation-of-eu-money-laundering-watchdog-ft/**

Commission (EC) would seek to strengthen AML and CFT[8] frameworks by conducting on-site inspections and examining the implementation of legislation.

So, in general, while automation and technology still have a central role, it is one driven by the human requirements of the KYC/AML landscape, namely managing large and expensive compliance teams. In this context, *outsourcing* and *augmenting* processes are becoming ever more important. As we explore later in this report, winning vendors are increasingly providing FIs with strong workflow for managing people and services as they operationalize.

Focus on COVID-19: the accelerant of digitization

Before the pandemic, FIs were adopting widespread digitization strategies, and increasingly coming to the conclusion that customer experience and onboarding times are both differentiators of performance and significant sources of cost. The COVID-19 crises has accelerated these previously existing trends. Banks are more digital in the way they operate, and rapid onboarding is even more vital to maintain a competitive edge and ensure customer satisfaction.

Banks' responsibilities around due diligence have always been demanding, but in the new COVID-19 environment they are increasingly harder to meet. The crisis has highlighted the need for faster real-time access to banking services for individuals and businesses in every jurisdiction, to gain loans and liquidity during the economic disruption. Likewise, many compliance teams are being stripped down, or working from home at limited capacity, and in several instances cyber defences have been compromised[9]. At a time when there are fewer staff in FIs, market abuse alerts are on the increase, and investigating every alert is not a viable option.

Nevertheless, FIs are expected to demonstrate to regulators that that they have robust processes in place to ensure that financial flows are legitimate. KYC information will need to be updated to keep pace. In March, the European Banking Authority (EBA) issued a policy statement[10] reminding banks to 'maintain effective systems and controls to ensure that the EU's financial system is not abused for money laundering or terrorist financing purposes' during the pandemic. It also called on regulators to support FIs' ongoing AML/CFT efforts, and reminded readers that financial crime remains unacceptable, even in times of crisis.

A need for efficiency

Historical issues around KYC and AML have arisen around:

- Model validation and benchmarking showing inconsistent results.
- Audit being a long, drawn-out process that only produces results several years after the incident itself.

There is now an understanding on both the regulatory and banking sides of the market that regulations are a significant cost drag on institutions that are required to be on the front line, providing finance and liquidity during the pandemic.

During this process, therefore, banks and regulators are invested in *efficiency*, and this has been reflected in banks' focus on model risk management and governance for their AML and KYC systems. In addition, despite the challenging circumstances, FIs must remain vigilant while onboarding new customers. In many cases, KYC and AML checks will have to be performed much more quickly and effectively. The US government, for example, attempted to disburse loans to small businesses (via the Small Business Administration Paycheck Protection Program [PPP]), yet lacked the staff to individually vet every business that applied. The process of checking loan applications was thus deferred to banks, which became responsible for disbursing monies[11].

But banks still need effective KYC/AML checks, and they simply cannot onboard fast enough. Faced with a tidal wave of loan applications, banks are having to undertake triage activities,

[8] *Countering the financing of terrorism.*
[9] *See, for example,* **https://www.verdict.co.uk/retail-banker-international/news/banks-see-a-238-surge-in-cyber-attacks-amid-covid-19/**
[10] *See* **https://eba.europa.eu/sites/default/documents/files/document_library/News%20and%20Press/Press%20Room/Press%20Releases/2020/EBA%20provides%20additional%20clarity%20on%20measures%20to%20mitigate%20the%20impact%20of%20COVID-19%20on%20the%20EU%20banking%20sector/Statement%20on%20actions%20to%20mitigate%20financial%20crime%20risks%20in%20the%20COVID-19%20pandemic.pdf**
[11] **https://home.treasury.gov/system/files/136/PPP-IFR-SBA-Loan-Review-Procedures-and-Related-Borrower-and-Lender-Responsibilities.pdf**

such as ensuring that only previously onboarded customers can access loans. There is consequently an inherent tension between legislation such as the Coronavirus Aid, Relief, and Economic Security (CARES) Act, which calls for speed in the disbursement of loans, and current AML laws and regulations, which involve detailed customer verification checks. As banks sprint to keep up in the process, calls are increasing for regulators to relax KYC/AML checks, to give banks more flexibility to serve non-customers as well as current ones. As a result of having fewer 'physical' staff in place because of COVID-19, many FIs have sped up their digitization projects and use of technology and large-scale workflow to manage the onboarding process. This is being performed without immediate recourse to the 'traditional solution' – hiring vast numbers of compliance and onboarding staff. We therefore expect compliance teams to remain broadly static for the duration of the crisis, with neither an increase nor a decrease in members.

The economic impact of COVID-19 will be long-lasting. Even the most resilient financial markets will be impacted by the broad restrictions on economic and social activities around the world. Programs like PPP in the US are unlikely to disappear any time soon, and the need for more of these types of programs will only continue even as restrictions begin to ease. Banks remain a critical channel for linking government finance and corporations. As these kinds of programs become more standardized, so too will the associated fraud, money laundering and compliance checks.

The importance of infrastructure as digitization accelerates

In general, the far-reaching consequences of the COVID-19 crisis are uncertain, but FIs' ability to cope with them will depend significantly on their technology infrastructure. The pandemic has highlighted the need for flexible technology architectures, and the effectiveness of FIs' efforts to mitigate their risk exposure will depend ultimately on their willingness to develop new technology strategies[12] and invest in systems and maintenance. While regulators are likely to give FIs short-term flexibility, they are unlikely to deviate significantly from ensuring that FIs have the capability to comply with KYC/AML legislation. In this context, FIs should not compromise on due-diligence measures, and reliable, trusted data[13] and flexible workflow tools are paramount in managing the onboarding process.

In a relatively short period of time, the nationwide lockdowns issued by governments around the world have created a huge shift in how businesses operate, individuals work, and consumers behave. For FIs, one of the most significant changes arising from COVID-19 has been the adoption and acceleration of digitization. COVID-19 has paved the way for digital transformation, as FIs have shifted to remote sales and service teams and launched digital outreach to customers to make flexible payment arrangements for loans and mortgages. For FIs of all sizes, the digitizing of operational processes may have always been in the pipeline, but it has now been accelerated because of the restrictions brought on by the pandemic. Firms that once mapped digital strategy in one to three-year phases have scaled their initiatives in a matter of days or weeks.

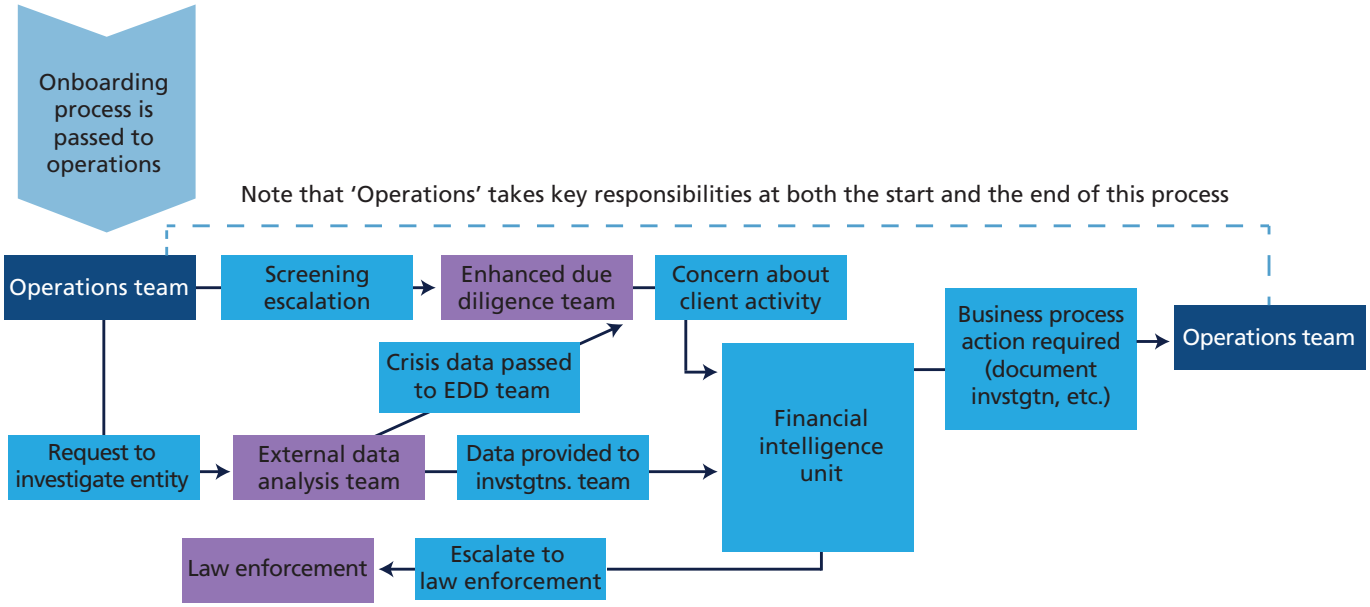
In general, COVID-19 has acted as a catalyst for change and accelerated pre-existing trends (such as the adoption of robotic process automation [RPA], workflow tools and cloud solutions). FIs dedicate significant time and resources to performing KYC assessments during onboarding, ongoing review intervals, and for enhanced due diligence (EDD) checks. All three components have inherently repetitive workflows, making them particularly suited to RPA solutions, which apply software tools to carry out repeatable tasks.

RPA typically involves 'screen scraping', developing macros and recording functionality to capture and replicate repetitive work. And although robotics processes generally operate without reconfigured core software, they must be integrated with underlying case management and the overall application to ensure effective controls. In addition, more and more vendors – notably analytics providers – are moving their offerings to the cloud. In general, it is becoming easier and cheaper for FIs to implement flexible workflow tools and services on the cloud.

In the post-pandemic future, digital technology will undoubtedly play a center-stage role. The pandemic has also exposed a clear digital divide: FIs that had already invested in digital capabilities have managed much better than those that had not. For many firms, continuity of operations now depends on their digital capabilities, and digital laggards risk a rocky future.

[12] *See the Chartis report 'Chartis Risk Bulletin: The Technology Impacts of COVID-19 - Market Overview and Guidance' for more information.*
[13] *See the Chartis report 'KYC/AML Data Solutions, 2020: Market and Vendor Landscape'.*

Figure 3. KYC/AML processes cross multiple business lines and requirements



Source: Chartis Research

In the following sections we examine the specifics of modern KYC/AML processes.

Analyzing KYC/AML processes: operations

If we establish that at the core of the compliance process are people solving problems with sign-off and responsibilities, what do these processes actually look like? Often, they cross multiple business lines and requirements (see Figure 3). Managing this web of requirements has led to the *operationalizing* of KYC/AML – in other words, managing the human element. This drives much of the efficiency gains of KYC/AML processes, and is made up of several key components.

Operational KYC/AML: outsourcing

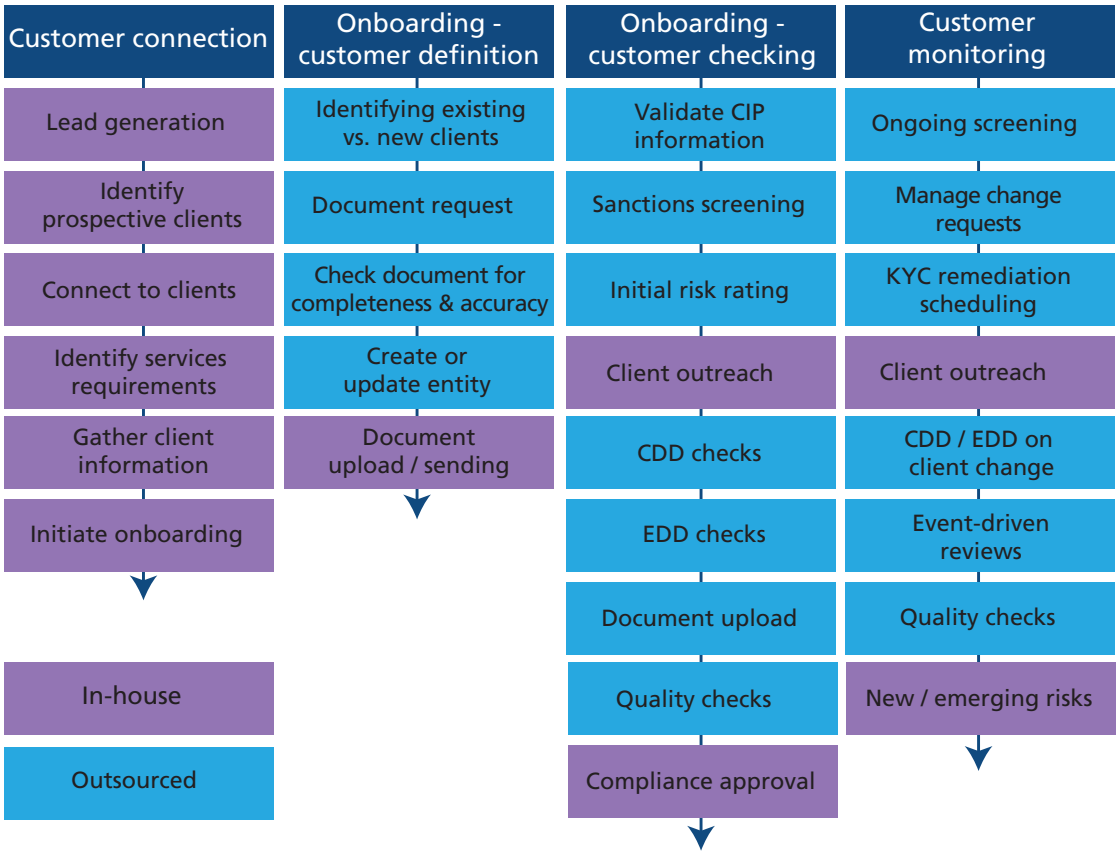
Outsourcing has become a key process element in KYC/AML systems in recent years. FIs are seeking to reduce in-house involvement in non-core AML compliance activities by outsourcing them to external providers. For many FIs, outsourcing is a cost-effective method of managing KYC/AML compliance and mitigating risk. The elements of KYC/AML activities that are outsourcing-friendly are usually those that are low-risk and involve fewer decision-making or 'human-centric' elements. Services companies, for example, are well-placed to manage labor-intensive and routine tasks such as customer due diligence (CDD), EDD and verifying customer IDs. These processes are typically redirected to in-house staff only when risk scores are particularly high.

Notably, any work carried out by an outsourcer does not remove the ultimate responsibility for KYC/AML from the FI. FIs must therefore remain aware of the tasks they outsource, to ensure they remain compliant with regulations. Final sign-off, or initiating contact with clients (to update documents, for example), must be done in-house. Any activities that include filing sensitive reports (such as internal investigations of suspicious behavior), are not conducive to outsourcing. These types of inquiries could involve employee interviews, document evaluations, and the preparation of reports, all of which require confidentiality and are challenging to outsource. Figure 4 illustrates the KYC/AML activities that are typically outsourced or performed in-house.

Operational KYC/AML: data

The second changing element of KYC/AML systems involves data processes. Good quality data is the foundation of accurate and reliable KYC/AML compliance. With accurate, easily accessible, secure and regularly updated data, FIs can confirm (with a degree of certainty) whether a given fact about an entity is true to a pre-packaged source when verifying identity. To guarantee accurate risk profiles for their retail and corporate customers, FIs' existing compliance processes involve many manual, repetitive and data-intensive tasks. And

Figure 4. Outsourced vs. in-house elements of KYC/AML processes



Source: Chartis Research

onboarding – a time-consuming and expensive process that depends on a large volume of accurate and robust data – is typically the most challenging element of the KYC process.

To clean and process large volumes of data, FIs have invested heavily in building large compliance teams, as well as technology and analytics. When sourcing KYC/AML data to screen potential customers (to establish and verify their identities and the related risks of conducting business with them), FIs rely heavily on publicly available information. This is often collected from registries or other sources that are independent of the counterparty itself. Data-cleaning processes occur either in-house or through an outsourcing service provided by third parties that is verified by FIs' compliance teams.

Given the complexity of the data and processes involved, FIs face a number of challenges in understanding the risks associated with individuals and businesses.

- **Data volumes**. Sanctions and politically exposed person (PEP) screening activities are especially prone to large numbers of false-positive alerts because of the number of lists, spellings, multiple aliases and diverse global character sets in existence. 'Bad data' – in the form of duplicate records, inconsistent data formats, and misplaced customer names in non-name fields – underpins false positives, but resolving the issue can be a highly complex task.

- **Unscalable and bottlenecked processes**. Sifting through vast amounts of data during the onboarding and ongoing monitoring of entities is a process that FIs struggle to scale fast enough to meet demand. This can then create bottlenecks within workflows: not all checks can be automated, as more difficult decisions must be validated by a compliance expert. This leads to further bottlenecks as cases become backlogged with busy compliance officers who cannot manage their workflow fast enough.

(These dynamics are covered in more detail in the Chartis report *KYC/AML Data Solutions, 2020: Market and Vendor Landscape*.)

Operational KYC/AML: workflow

The third key change is in workflow. The lifecycle applications of KYC and due-diligence processes – whether during onboarding or ongoing monitoring – are managed by various teams across the organization. FIs should have flexible workflow engines and tools that can be fully customized by the compliance team itself when it assigns and manages tasks. Configurable workflow tools allow FIs to perform their own identification and verification processes to suit their individual business requirements. And when outsourcing elements of KYC/AML processes, FIs require flexible workflow and application programming interfaces (APIs) to help manage tasks that can be automated.

Operational KYC/AML: analytics

Analytics typically focus on integrating data into the workflow, providing quick and reliable information or automating specific use cases. Analytics tools often include entity resolution and graph analytics. Entity resolution resolves identities and detects relationships, using automated systems that can scan and match large amounts of data in a timely way, to identify customers and prevent duplicate accounts or impersonation. Entity resolution helps FIs comply with various KYC/AML regulations and sanctions screening activities, by providing higher-quality data to improve risk profiling and scoring.

Graph analytics, also known as network analysis, is a category of tools that apply algorithms to understand, codify and visualize relationships between entities. Because graph analytics techniques can reveal insights about the strength and direction of relationships, they continue to win market share in the high-volume, low-complexity retail section of the market, where they are used to manage entity resolution. Rich rules libraries for defining complex entities are especially effective in wholesale and corporate KYC applications.

3. Vendor landscape

The market shifts outlined in the previous section – especially the growing need for digitization and speed across the KYC/AML solution landscape – are driving changes in the relevant technology solutions offered by vendors. As their customers' behavior changes, many FIs are reassessing their digital initiatives to ensure that they are as good as, or better, than those of their competitors. When piloting new digital initiatives, very few FIs can achieve the scale and speed now required because of the COVID-19 crisis. So increasingly they are turning to technology vendors rather than in-house options to accelerate their digital transformation and speed up the onboarding process.

In accommodating FIs' requirements, vendors have sharpened their focus on their data-gathering and workflow capabilities. Increasingly, winning vendors are providing solutions that offer scalability, usability and data security for KYC/AML processes. This includes cloud-based deployments and managed services capabilities.

Key trends

KYC onboarding and AML transaction monitoring at the forefront of the solutions market

According to a recent study[14], 41% of businesses plan to change their banking provider because they have received poor service during the pandemic. Of 200 business decision makers across large and medium-sized companies, 42% had to wait for more than two weeks for a business loan application, while 46% experienced significant delays during the onboarding process. In addition, 40% expressed dissatisfaction with their bank's digital services capabilities. The economic and social restrictions brought on by COVID-19 have underlined the value of onboarding procedures that can be accessed rapidly and remotely. Several vendors have rolled out specific solutions targeted at COVID-19 legislation or relief programs such as the CARES Act in the US. Because of the increased attention on KYC and onboarding, vendors have started to focus more on what a successful solution comprises. This has led to the formation of strategies around measuring productivity by FIs. The time-to-profile, analyst effort, accuracy and success of onboarding are all critical factors for FIs in overcoming their new challenges.

More data-provision capabilities

More and more vendors – even those that historically have had an analytics and case-management focus – are specializing in providing data-provision capabilities. Increasingly, the lines between data providers and software and analytics vendors are becoming blurred. As FIs ingest data from ever more sources, vendors have grown to accommodate the change, often meeting specific requirements for different business lines. Successful data-provision capabilities can become industry standards, benefiting from network effects to grow in size and subsequently reinvest in data science and analytics capabilities to grow further. By their nature, data-service offerings are more 'binary' than analytics offerings (put bluntly, within a given vertical you either provide data or you don't). As a result, vendors with strengths across multiple data verticals tend to be emphasized in the landscape. This is compounded by the network effects of data acquisition, whereby market-leading vendors in each data vertical tend to consolidate their position.

Acquiring more proprietary data is one of the most effective paths to profitability in risk technology, and is encouraging vendors to specialize. Those that specialize in specific types of data (such as ID data, negative news and biometrics) can establish themselves as the industry standard for that type of information. In the fight against COVID-19, real-time information, especially mobile phone location data, is a critical source that governments can use to try and control the pandemic. By providing public records and people-locating solutions, data providers are well placed to help identify and locate individuals who may be at high risk of infectious disease.

Partnerships and deployment strategies remain key

In the fragmented KYC/AML solutions market, competition requires cooperation. In a key dynamic in the KYC/AML landscape, many vendors are building strong partnerships with services companies and other technology firms to augment their solutions. Vendors are assessing their own capabilities and creating more defined relationships

[14] *See* **https://www.verdict.co.uk/switch-banking-provider/**

with one another, because partnerships allow access to new markets and decrease time and development costs. A packaged KYC provider, for example, could partner with a vendor that specializes in data analytics, to lower processing times and boost scalability. APIs and connectors are becoming more standardized to ensure that deployments are as modular as possible. APIs, which are flexible, organized and well-documented, can more easily be integrated with other vendors' core infrastructure and successfully meet new requirements. In addition, hybrid services and technology are becoming more common. We are seeing this approach from several vendors that provide their own technology solutions alongside large and well-developed teams of system integrators. Via managed services and consulting vendors can help users manage entity data, screening and alerts.

Geographical expansion

Over the last few years, the location of the most significant KYC/AML expenditure has shifted. As highlighted in LexisNexis Risk Solution's 2020 global cost of compliance study[15], large fines are no longer ordered mainly by US regulators, and penalties from regulators in other regions – especially Europe – are now becoming bigger and more frequent. This has resulted in a move away from vendors that previously dominated this market, and which had a strong presence in the US. In addition, there has been a broader but less dramatic expansion in the geographical focus of KYC/AML solutions. Vendors have seen gains in regions (such as Barbados and the Cayman Islands) that previously did not have a large KYC/AML presence.

General technology trends

The key technology trends in the KYC/AML market include the following.

- **Cloud deployments are becoming more common**. Users are seeing several important advantages in cloud solutions, notably low entry costs, scalability and speed to market. Cloud computing also provides flexible data storage for analytics, customer relationship management, reference data and regulatory reporting services. Cloud deployments are implemented at different parts of the KYC/AML stack. For example, sanctions screening processes have traditionally been managed by cloud providers, and FIs have used APIs to check against online repositories of sanctioned entities. Many other elements of financial crime solutions are moving to the cloud. Nevertheless, in some areas, such as transaction monitoring, the importance of data security and the need for rapid processing mean that on-premise deployments dominate.

- **Specific hardware is being deployed as a solution strategy**. Graph databases for KYC, for example, are being deployed more often as part of a vendor solution set. Graph databases employ graph structures for queries, using nodes, edges and properties to represent and store data. They underpin graph analytics, identity resolution and enhanced workflows.

- **A wider variety of onboarding data is required**. The COVID-19 pandemic has accelerated the transition to digital methods of customer identity verification and validation during the onboarding process. Biometrics and facial recognition have been key tools in onboarding customers quickly and remotely, although these innovations can have wide-reaching regulatory impacts. Firms outside Illinois, for example, have already been sued under the Illinois Biometric Information Privacy Act (BIPA)[16].

- **A wake-up call on advanced analytics**. Vendors and services firms have often over-promised on their offerings, creating a cycle of replacement and disillusionment, and FIs now want tangible results. Driven by demand for interpretation and explicability, users increasingly require analytics-specific solutions to provide more depth and scalability.

New entrants and changes in the marketplace

In addition, the market is receiving more attention from 'traditional' business process workflow vendors, although historically these have been integrators or have partnered with other vendors with KYC/AML capabilities. We are seeing big workflow and commercial vendors establishing partnerships with vendors that provide KYC functionality. Workflow vendors are also providing capabilities (such as RPA tools) within their financial crime risk-management solutions.

[15] **https://risk.lexisnexis.com/global/en/insights-resources/research/the-true-cost-of-aml-compliance-european-survey**
[16] *See, for example,* **https://news.bloomberglaw.com/privacy-and-data-security/insight-illinois-biometric-privacy-law-has-nationwide-potential-in-pandemic**

Meanwhile, expansion into new areas such as FinTech can expose unexpected risks. KYC and AML requirements are continuing to expand into adjacent industries. Increasingly, FinTech firms (such as payment processors and wallet providers) are required to provide their own KYC/AML processes, and financialized corporate firms also now require greater due diligence in terms of who they do business with. Frequently, vendors are finding pathways to provide solutions for these entities via partnerships with other commercial vendors or services firms. This raises the chance of third-party risk, whereby firms could lose track of the level of compliance of all the firms involved in their payment processing.

Chartis RiskTech Quadrant® and vendor capabilities for KYC solutions, 2020

Quadrant dynamics

One notable element of this quadrant is the sheer number of vendors it contains, which has increased significantly. The number of vendors in the category leader space has also increased significantly, as there are a number of routes to category-leader status: building out existing advanced KYC capabilities, or expanding client lifecycle management tools. The mixture of technology and services also changes from firm to firm. Some provide a focused, pre-packaged technology stack, while others provide more of a services-based offering reinforced by technology.

Notably, the vendors in the quadrant address many different markets, so some do not actually compete directly with each another. As a result, separate firms have achieved market-leading positions within corporate and investment banking, retail, or wealth management.

Data remains a key part of the KYC process, and firms with significant data assets achieved the highest market potential scores. The dynamics of this market are addressed in more detail in the Chartis report *KYC/AML Data Solutions, 2020: Market and Vendor Landscape*, but it is notable here that the ability to build out entity relationships with proprietary data remains key to a durable market presence.

Onboarding and workflow capabilities have increased significantly across the board as more vendors have acknowledged these as key challenges for FIs. Consequently, many vendors that were previously specialists have been building out their case-management capabilities, either through partnerships or specific software improvements. However, it is still possible to develop a market-leading position as a component vendor, and capabilities such as entity resolution remain highly important.

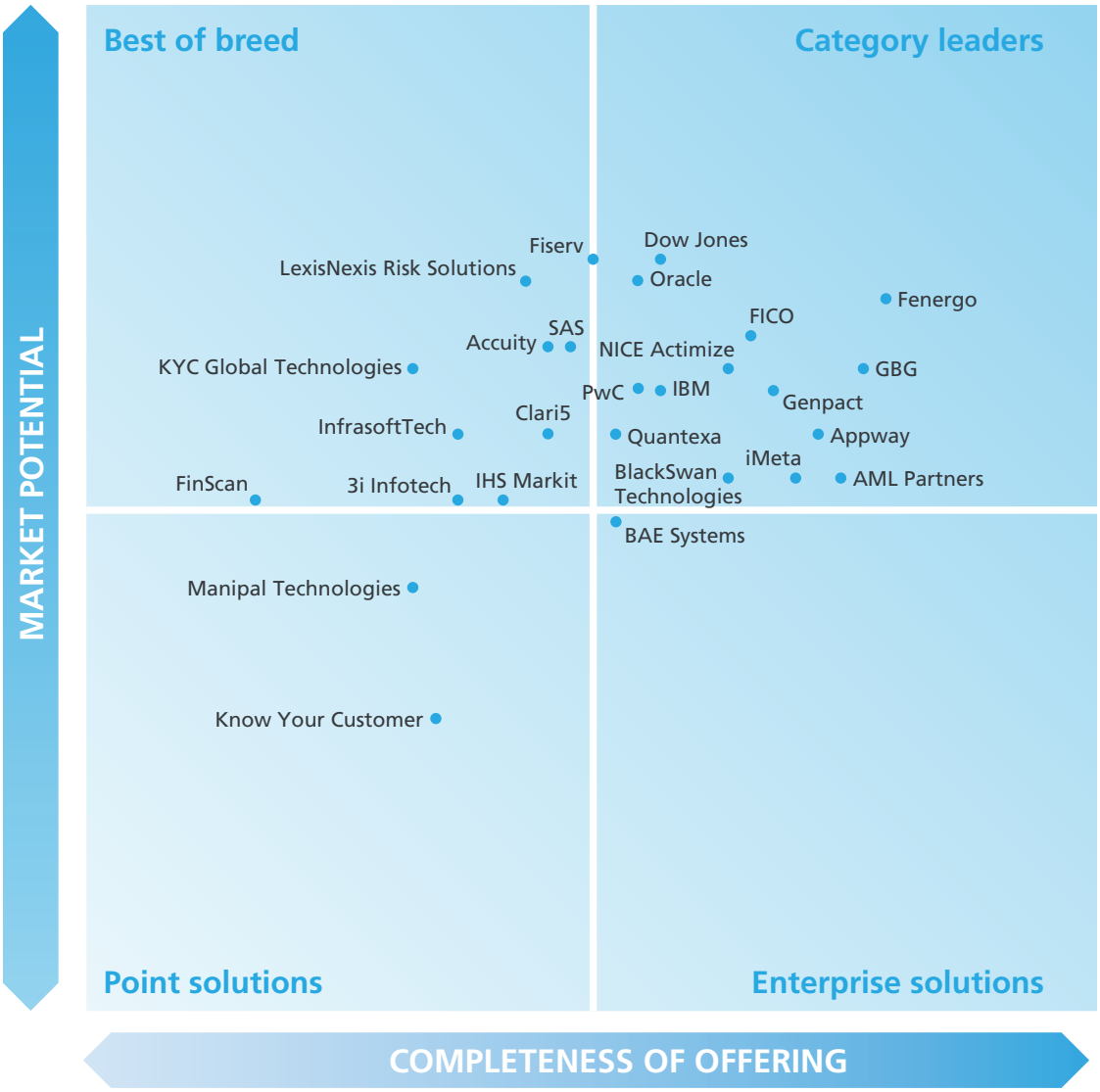
Figure 5 illustrates Chartis' view of the vendor landscape for KYC solutions. Table 1 lists the completeness of offering and market potential criteria we used to assess the vendors. Table 2 lists the vendor capabilities in this area.

Table 1: Assessment criteria for vendors of KYC solutions, 2020

Completeness of offering	Market potential
• Entity resolution	• Customer satisfaction
• Reporting and dashboarding	• Market penetration
• KYC risk scores	• Growth strategy
• Customer profile enrichment with additional data	• Financials
• Customer onboarding	• Business model
• Workflow engine	

Source: Chartis Research

Figure 5: RiskTech Quadrant® for KYC solutions, 2020



Source: Chartis Research

Table 2: Vendor capabilities for KYC solutions, 2020

Vendor	Entity resolution	Reporting and dashboarding	KYC risk scores	Customer profile enrichment with additional data	Customer onboarding	Workflow engine
3i Infotech	*	**	**	*	***	***
Accuity	**	**	**	****	**	*
AML Partners	**	***	**	**	****	****
Appway	*	***	**	**	****	****
BAE Systems	**	**	**	**	**	**
BlackSwan Technologies	****	**	**	**	**	**
Clari5	**	**	**	**	**	**
Dow Jones	**	**	**	****	**	**
Fenergo	***	**	***	**	***	***
FICO	***	**	**	***	**	**
FinScan	*	**	*	**	*	*
Fiserv	**	**	**	***	**	*
GBG	**	***	**	***	***	***
Genpact	**	**	**	**	***	***
IBM	**	**	**	***	*	***
IHS Markit	**	**	*	****	**	*
iMeta	**	**	***	**	***	**
InfrasoftTech	*	**	**	*	***	**
KnowYour Customer	*	**	**	**	**	**
KYC Global Technologies	*	**	**	***	**	**

*Key: **** = Best-in-class capabilities; *** = Advanced capabilities; ** = Meets industry requirements; * = Partial coverage/component capability*
Source: Chartis Research

Table 2a: Vendor capabilities for KYC solutions, 2020 (continued)

Vendor	Entity resolution	Reporting and dashboarding	KYC risk scores	Customer profile enrichment with additional data	Customer onboarding	Workflow engine
Lexis Nexis Risk Solutions	**	**	**	****	**	*
Manipal Technologies	*	**	**	*	**	**
NICE Actimize	**	***	**	**	***	***
Oracle	***	**	**	**	**	**
PwC	**	**	**	**	***	**
Quantexa	****	**	**	*	***	*
SAS	**	***	**	**	**	**

*Key: **** = Best-in-class capabilities; *** = Advanced capabilities; ** = Meets industry requirements; * = Partial coverage/component capability*
Source: Chartis Research

Chartis RiskTech Quadrant® and vendor capabilities for AML solutions, 2020

Quadrant dynamics

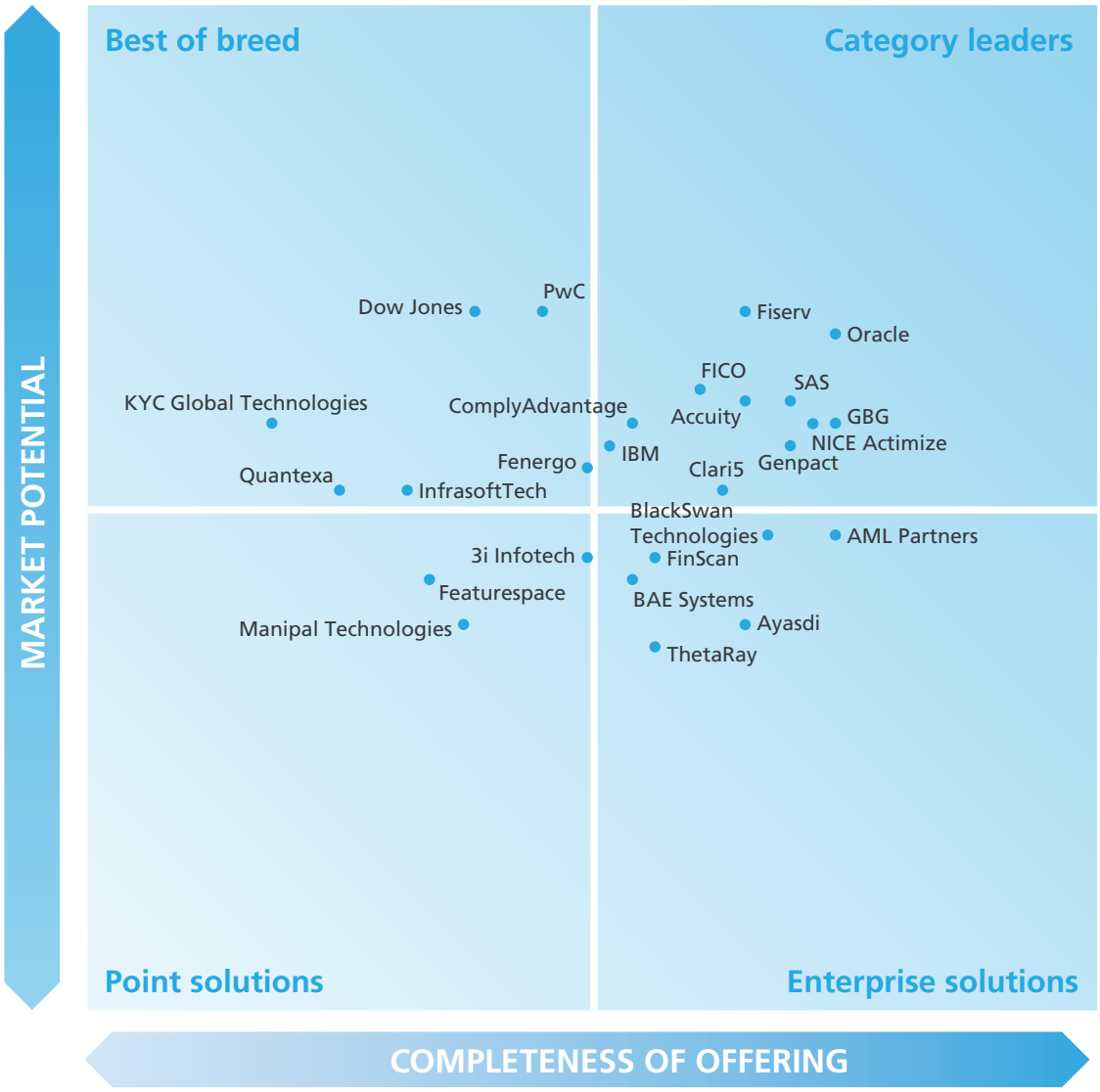
As in the KYC space, a key takeaway from the AML quadrant is the growing number of vendors in the space, and the increasing number of category leaders. This is the result of specialist vendors emerging and consolidating their position in the AML space, and the growth of competitors that are challenging the dominant players. For challengers, the key capabilities are typically transaction monitoring and case management. Vendors in the category leader quadrant also represent a wider variety of geographies than in past iterations of this quadrant, including those which are expanding out from a traditional US focus to concentrate on India, China and Europe.

While providing specific analytics capabilities is a challenge in the current component driven environment, several vendors have gained positions in the enterprise solutions category, by expanding their core capabilities to offer specialisms in either transaction monitoring or case management.

We have also seen specialist capabilities driving significant market presence. As a result of the 'component-based' dynamic in KYC and AML solutions, some vendors have been able to build strong client portfolios. Typically, the firms who have had success in building out their market presence using specialist capabilities have been sanctions-screening and data specialists (which retain a strong presence in the landscape), but we have recently seen strong growth from specialist vendors providing capabilities such as entity resolution.

Figure 6 illustrates Chartis' view of the vendor landscape for AML solutions. Table 3 lists the completeness of offering and market potential criteria we used to assess the vendors. Table 4 lists the vendor capabilities in this area.

Figure 6: RiskTech Quadrant® for AML solutions, 2020



Source: Chartis Research

Table 3: Assessment criteria for vendors of AML solutions, 2020

Completeness of offering	Market potential
• Name and watchlist screening capabilities	• Customer satisfaction
• Breadth of name screening sources offered	• Market penetration
• Transaction monitoring capabilities	• Growth strategy
• Regulatory compliance reporting and controls	• Financials
• Alert/case management	• Business model
• Advanced analytics	
• Visualizations and dashboarding	

Source: Chartis Research

Table 4: Vendor capabilities for AML solutions, 2020

Vendor	Name & watchlist screening	Breadth of name screening sources	Transaction monitoring	Regulatory compliance reporting & controls	Alert/ case mngmnt	Advanced analytics	Visualizations & dashboarding
3i Infotech	**	**	***	**	***	**	**
Accuity	****	***	**	**	**	**	**
AML Partners	**	**	**	***	****	**	***
Ayasdi	**	*	***	**	**	****	***
BAE Systems	**	**	**	**	***	**	**
BlackSwan Technologies	**	**	**	**	**	***	***
Clari5	**	**	****	**	**	**	**
ComplyAdvantage	***	**	**	**	**	**	**
Dow Jones	**	****	*	**	*	**	**
Featurespace	*	*	***	**	*	**	***
Fenergo	**	**	*	****	**	**	**
FICO	**	**	**	**	***	**	**
FinScan	***	**	**	**	**	***	**

*Key: **** = Best-in-class capabilities; *** = Advanced capabilities; ** = Meets industry requirements; * = Partial coverage/component capability*
Source: Chartis Research

Table 4a: Vendor capabilities for AML solutions, 2020 (continued)

Vendor	Name & watchlist screening	Breadth of name screening sources	Transaction monitoring	Regulatory compliance reporting & controls	Alert/ case mngmnt	Advanced analytics	Visualizations & dashboarding
Fiserv	**	**	***	**	***	**	**
GBG	**	**	***	***	***	**	***
Genpact	**	**	***	**	***	**	***
IBM	**	**	***	**	*	**	***
InfrasoftTech	**	**	**	**	**	*	*
KYC Global Technologies	**	**	*	**	**	*	**
Manipal Technologies	**	**	**	**	**	**	*
NICE Actimize	**	**	**	***	****	***	***
Oracle	**	**	**	***	***	***	***
PwC	*	*	**	****	**	**	**
Quantexa	*	*	**	**	**	***	***
SAS	**	**	****	**	**	***	***
ThetaRay	**	**	***	**	*	***	**

*Key: **** = Best-in-class capabilities; *** = Advanced capabilities; ** = Meets industry requirements; * = Partial coverage/component capability*
Source: Chartis Research

4. Appendix A: Actions and fines from regulators: ongoing developments

Fines on the increase, across the globe

Between 2008 and 2019 regulators issued $36 billion worth of fines globally for non-compliance with AML, KYC and sanctions regulations[17]. According to a research report from Fenergo that examines fines and enforcement actions on FIs, fines in 2019 were second only to 2015 by monetary value: $10 billion of fines were issued to institutions for non-compliance with AML, KYC and sanctions regulations. Sanctions violations, which were all issued by US regulators, made up 37% of all global penalties, which amounted to $3.76 billion. Amid global trade tensions, the fines were meted out to European FIs for violating sanctions for countries such as Iran, Cuba, North Korea, Sudan, Libya and Myanmar.

One notable trend is the shift away from US regulators as the main source of large fines. Fines are now more globally distributed. In 2019, European regulatory bodies issued $5.7 billion of fines – the largest amount by monetary value – for violations of KYC/AML, GDPR and Markets in Financial Instruments Directive (MiFID) I regulations. UBS received a $5.1 billion fine after being convicted of helping wealthy French clients evade the tax authorities[18]. In an indication of just how hard a line regulators are taking on financial misconduct and AML violations, the fine exceeded the firm's net profit in 2018. Danske Bank has been at the center of one of the largest money laundering incidents in Europe, after revelations that it channeled €2 billion of suspicious transactions through its Estonian branch from 2007 to 2015[19].

UniCredit paid out $1.3 billion for processing payments between 2007 and 2011 that were in violation of US government sanctions several countries including Iran, Cuba and Libya[20]. Standard Chartered was fined $1.1 billion by UK and US regulators for inadequate money-laundering controls and sanctions breaches[21]. Deutsche Bank paid $630 million in fines to UK and US regulators in 2017 for its 'mirror trading scandal', which laundered $10 billion out of Russia[22]. As part of the trading scheme, which

Spotlight on regulatory expansion

Barbados is on the Financial Action Task Force's (FATF's) list of countries that have been identified as having strategic AML deficiencies, and the EC has recently included Barbados as one of 20 countries on its new AML and terrorism-financing blacklist. In response, the government of Barbados has made a commitment at the highest political level to work with the FATF and the Caribbean Financial Action Task Force (CFATF) to strengthen the effectiveness of its AML/CFT regime. Since 2017, Barbados has made progress on several of its mutual evaluation report (MER) recommendations to improve technical compliance and effectiveness, such as updating the country's national risk assessment and developing mitigating measures.

Similarly, the **Cayman Islands** has implemented the FATF's 40 recommendations on preventing money laundering and countering terrorist financing. Notable changes include removing the equivalent jurisdiction list, applying a 10% beneficial ownership threshold, and complying with sanctions lists.

The measures to combat money laundering taken by many countries that have previously had weak procedures in place has been driven mainly by the global evolution of KYC and AML regimes in 2019. Regulatory authorities such as FinCEN, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) and the EC have enforced stricter KYC/AML measures, especially for CDD and UBO.

[17] **https://www.fenergo.com/resources/reports/another-fine-mess-global-research-report-financial-institution-fines.html**
[18] **https://www.marketwatch.com/story/swiss-bank-ubs-ordered-to-pay-42-billion-in-fines-2019-02-20**
[19] **https://www.bloomberg.com/news/articles/2020-01-03/danske-faces-2-billion-in-fines-for-laundering-case-jyske-says**
[20] **https://www.reuters.com/article/us-unicredit-sanctions-settlement-exclus/italys-unicredit-to-pay-1-3-billion-to-settle-u-s-sanctions-probe-idUSKCN1RR1TK**
[21] **https://www.theguardian.com/business/2019/apr/09/standard-chartered-fined-money-laundering-sanctions-breaches**
[22] **https://www.theguardian.com/business/2017/jan/31/deutsche-bank-fined-630m-over-russia-money-laundering-claims**

operated from 2011 to 2015, Russian clients bought securities in rubles through the bank's Moscow office, and sold identical ones for foreign currency via the bank's London office. The proceeds of the shares often ended up in offshore banking centers such as Cyprus.

After a series of banking scandals in Europe, in which EMEA-based FIs received 97% of all fines issued globally in 2019, the EC set out plans to create a new AML enforcement body. As enforcement across Europe can be patchy, the new body would seek to strengthen AML directives by conducting on-site inspections and assessing the implementation of legislative requirements.

The Fifth Anti-Money Laundering Directive

The Fifth Anti-Money Laundering Directive (5AMLD), an EU directive that came into force in January 2020, is designed to prevent the use of the financial system for money laundering and terrorist financing. The 5AMLD builds on the regulatory regime applied under its predecessor, the Fourth Anti-Money Laundering Directive (4AMLD). The main additional requirements of the 5AMLD include:

- **Obligated entities**. The 5AMLD extends the sectors that are now obligated entities:
    - Providers of virtual currencies and custodian wallets.
    - Art traders.
    - Those that provide similar services to auditors, external accountants and tax advisors as a principal business or professional activity.
    - Estate agents that act as intermediaries in the letting of property for which the monthly rent is equivalent to €10,000 or more.
- **Pre-paid cards**. Remote payment transactions that exceed €50 are now subject to CDD measures; the threshold has been reduced from €100. In addition, FIs must consider mitigating risk measures when managing customers that have an electronically stored amount of €150. This is a change from the previous threshold of €250 established by the 4AMLD.
- **PEPs**. The 5AMLD requires EU member states and any international organizations accredited to it to compile up-to-date lists of exact roles that qualify as prominent public functions. The EC will assemble and make publicly available a single list of all prominent public functions.
- **CDD**. During onboarding, firms must identify and verify customers based on data from a reliable independent source. Where available, this should also include means of electronic identification that have been approved by national authorities.
- **Beneficial ownership registers**. The 5AMLD requires all member states to establish a centralized register of the UBOs of companies, and to make this information publicly available.
- **EDD**. Firms that conduct business with customers from high-risk countries are now required to execute EDD measures aimed precisely at addressing the deficiencies in those countries' AML protections and the money laundering risks they present.
- **Information sharing**. Centralized automated mechanisms will permit financial intelligence units (FIUs) and similar authorities to identify account holders in a timely manner. FIUs will now be able to obtain any information required from an obliged entity, even without the creation of a prior suspicious transaction report.

5. Appendix B: RiskTech Quadrant® methodology

Chartis is a research and advisory firm that provides technology and business advice to the global risk management industry. Chartis provides independent market intelligence regarding market dynamics, regulatory trends, technology trends, best practices, competitive landscapes, market sizes, expenditure priorities, and mergers and acquisitions. Chartis' RiskTech Quadrant® reports are written by experienced analysts with hands-on experience of selecting, developing, and implementing risk management systems for a variety of international companies in a range of industries including banking, insurance, capital markets, energy, and the public sector.

Chartis' research clients include leading financial services firms and Fortune 500 companies, leading consulting firms, and risk technology vendors. The risk technology vendors that are evaluated in the RiskTech Quadrant® reports can be Chartis clients or firms with whom Chartis has no relationship. Chartis evaluates all risk technology vendors using consistent and objective criteria, regardless of whether or not they are a Chartis client.

Where possible, risk technology vendors are given the opportunity to correct factual errors prior to publication, but cannot influence Chartis' opinion. Risk technology vendors cannot purchase or influence positive exposure. Chartis adheres to the highest standards of governance, independence, and ethics.

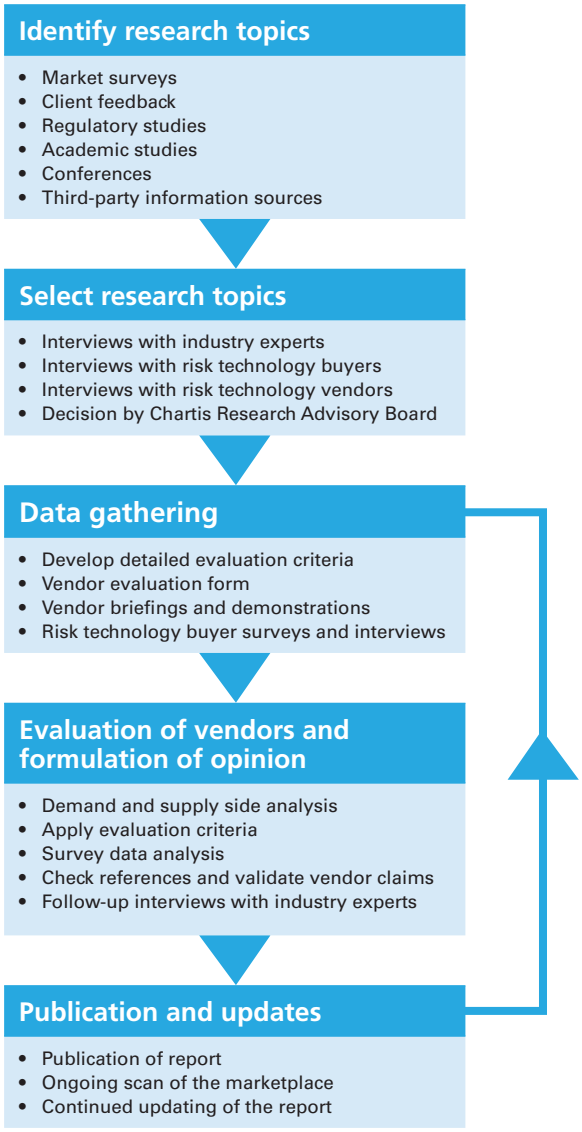
Inclusion in the RiskTech Quadrant®

Chartis seeks to include risk technology vendors that have a significant presence in a given target market. The significance may be due to market penetration (e.g. large client-base) or innovative solutions. Chartis does not give preference to its own clients and does not request compensation for inclusion in a RiskTech Quadrant® report. Chartis utilizes detailed and domain-specific 'vendor evaluation forms' and briefing sessions to collect information about each vendor. If a vendor chooses not to respond to a Chartis vendor evaluation form, Chartis may still include the vendor in the report. Should this happen, Chartis will base its opinion on direct data collated from risk technology buyers and users, and from publicly available sources.

Research process

The findings and analyses in the RiskTech Quadrant® reports reflect our analysts' considered opinions, along with research into market trends, participants, expenditure patterns, and best practices. The research lifecycle usually takes several months, and the analysis is validated through several phases of independent verification. Figure 7 below describes the research process.

Figure 7: RiskTech Quadrant® research process



Source: Chartis Research

Chartis typically uses a combination of sources to gather market intelligence. These include (but are not limited to):

- **Chartis vendor evaluation forms.** A detailed set of questions covering functional and non-functional aspects of vendor solutions, as well as organizational and market factors. Chartis' vendor evaluation forms are based on practitioner level expertise and input from real-life risk technology projects, implementations, and requirements analysis.
- **Risk technology user surveys.** As part of its ongoing research cycle, Chartis systematically surveys risk technology users and buyers, eliciting feedback on various risk technology vendors, satisfaction levels, and preferences.
- **Interviews with subject matter experts.** Once a research domain has been selected, Chartis undertakes comprehensive interviews and briefing sessions with leading industry experts, academics, and consultants on the specific domain to provide deep insight into market trends, vendor solutions, and evaluation criteria.
- **Customer reference checks.** These are telephone and/or email checks with named customers of selected vendors to validate strengths and weaknesses, and to assess post-sales satisfaction levels.
- **Vendor briefing sessions.** These are face-to-face and/or web-based briefings and product demonstrations by risk technology vendors. During these sessions, Chartis experts ask in-depth, challenging questions to establish the real strengths and weaknesses of each vendor.
- **Other third-party sources.** In addition to the above, Chartis uses other third-party sources of information such as conferences, academic and regulatory studies, and collaboration with leading consulting firms and industry associations.

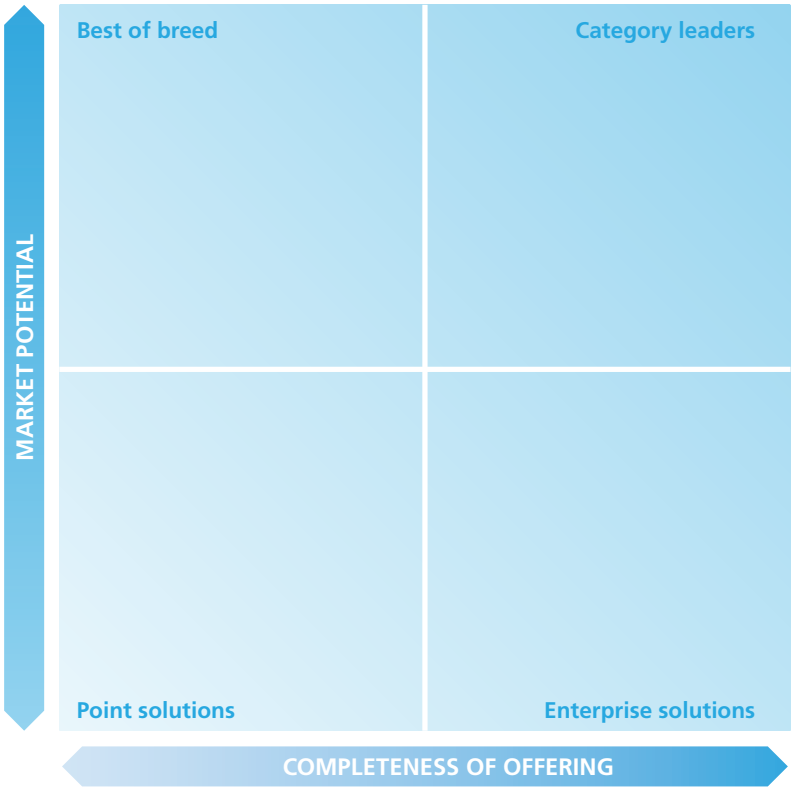
Evaluation criteria

The RiskTech Quadrant® (see Figure 8) evaluates vendors on two key dimensions:

1. Completeness of offering

2. Market potential

Figure 8: RiskTech Quadrant®



Source: Chartis Research

We develop specific evaluation criteria for each piece of quadrant research from a broad range of overarching criteria, outlined below. By using domain-specific criteria relevant to each individual risk, we can ensure transparency in our methodology, and allow readers to fully appreciate the rationale for our analysis.

Completeness of offering

- **Depth of functionality.** The level of sophistication and amount of detailed features in the software product (e.g. advanced risk models, detailed and flexible workflow, domain-specific content). Aspects assessed include: innovative functionality, practical relevance of features, user-friendliness, flexibility, and embedded intellectual property. High scores are given to those firms that achieve an appropriate balance between sophistication and user-friendliness. In addition, functionality linking risk to performance is given a positive score.
- **Breadth of functionality.** The spectrum of requirements covered as part of an enterprise risk management system. This will vary for

each subject area, but special attention will be given to functionality covering regulatory requirements, multiple risk classes, multiple asset classes, multiple business lines, and multiple user types (e.g. risk analyst, business manager, CRO, CFO, Compliance Officer). Functionality within risk management systems and integration between front-office (customer-facing) and middle/back office (compliance, supervisory, and governance) risk management systems are also considered.

- **Data management and technology infrastructure.** The ability of risk management systems to interact with other systems and handle large volumes of data is considered to be very important. Data quality is often cited as a critical success factor and ease of data access, data integration, data storage, and data movement capabilities are all important factors. Particular attention is given to the use of modern data management technologies, architectures, and delivery methods relevant to risk management (e.g. in-memory databases, complex event processing, component-based architectures, cloud technology, software-as-a-service). Performance, scalability, security, and data governance are also important factors.

- **Risk analytics.** The computational power of the core system, the ability to analyze large amounts of complex data in a timely manner (where relevant in real time), and the ability to improve analytical performance are all important factors. Particular attention is given to the difference between 'risk' analytics and standard 'business' analytics. Risk analysis requires such capabilities as non-linear calculations, predictive modeling, simulations, scenario analysis, etc.

- **Reporting and presentation layer.** The ability to present information in a timely manner, the quality and flexibility of reporting tools, and ease of use are important for all risk management systems. Particular attention is given to the ability to do ad-hoc 'on-the-fly' queries (e.g. what-if-analysis), as well as the range of 'out-of-the-box' risk reports and dashboards.

Market potential

- **Business model**. Includes implementation and support and innovation (product, business model and organizational). Important factors include size and quality of implementation team, approach to software implementation, and post-sales support and training. Particular attention is given to 'rapid' implementation methodologies and 'packaged' services offerings. Also evaluated are new ideas, functionality and technologies to solve specific risk management problems. Speed to market, positioning, and translation into incremental revenues are also important success factors in launching new products.

- **Market penetration**. Volume (i.e. number of customers) and value (i.e. average deal size) are considered important. Rates of growth relative to sector growth rates are also evaluated. Also covers brand awareness, reputation, and the ability to leverage current market position to expand horizontally (with new offerings) or vertically (into new sectors).

- **Financials**. Revenue growth, profitability, sustainability, and financial backing (e.g. the ratio of license to consulting revenues) are considered key to scalability of the business model for risk technology vendors.

- **Customer satisfaction**. Feedback from customers is evaluated, regarding after-sales support and service (e.g. training and ease of implementation), value for money (e.g. price to functionality ratio) and product updates (e.g. speed and process for keeping up to date with regulatory changes).

- **Growth strategy**. Recent performance is evaluated, including financial performance, new product releases, quantity and quality of contract wins, and market expansion moves. Also considered are the size and quality of the sales force, sales distribution channels, global presence, focus on risk management, messaging, and positioning. Finally, business insight and understanding, new thinking, formulation and execution of best practices, and intellectual rigor are considered important.

Quadrant descriptions

Point solutions

- Point solutions providers focus on a small number of component technology capabilities, meeting a critical need in the risk technology market by solving specific risk management problems with domain-specific software applications and technologies.
- They are often strong engines for innovation, as their deep focus on a relatively narrow area generates thought leadership and intellectual capital.
- By growing their enterprise functionality and utilizing integrated data management, analytics and BI capabilities, vendors in the point solutions category can expand their completeness of offering, market potential and market share.

Best-of-breed

- Best-of-breed providers have best-in-class point solutions and the ability to capture significant market share in their chosen markets.
- They are often distinguished by a growing client base, superior sales and marketing execution, and a clear strategy for sustainable, profitable growth. High performers also have a demonstrable track record of R&D investment, together with specific product or 'go-to-market' capabilities needed to deliver a competitive advantage.
- Focused functionality will often see best-of-breed providers packaged together as part of a comprehensive enterprise risk technology architecture, co-existing with other solutions.

Enterprise solutions

- Enterprise solutions providers typically offer risk management technology platforms, combining functionally-rich risk applications with comprehensive data management, analytics and BI.
- A key differentiator in this category is the openness and flexibility of the technology architecture and a 'toolkit' approach to risk analytics and reporting, which attracts larger clients.
- Enterprise solutions are typically supported with comprehensive infrastructure and service capabilities, and best-in-class technology delivery. They also combine risk management content, data and software to provide an integrated 'one-stop-shop' for buyers.

Category leaders

- Category leaders combine depth and breadth of functionality, technology and content with the required organizational characteristics to capture significant share in their market.
- Category leaders demonstrate a clear strategy for sustainable, profitable growth, matched with best-in-class solutions and the range and diversity of offerings, sector coverage and financial strength to absorb demand volatility in specific industry sectors or geographic regions.
- Category leaders will typically benefit from strong brand awareness, global reach and strong alliance strategies with leading consulting firms and systems integrators.

6. How to use research and services from Chartis

In addition to our flagship industry reports, Chartis offers customized information and consulting services. Our in-depth knowledge of the risk technology market and best practice allows us to provide high-quality and cost-effective advice to our clients. If you found this report informative and useful, you may be interested in the following services from Chartis.

For risk technology buyers

If you are purchasing risk management software, Chartis's vendor selection service is designed to help you find the most appropriate risk technology solution for your needs.

We monitor the market to identify the strengths and weaknesses of the different risk technology solutions, and track the post-sales performance of companies selling and implementing these systems. Our market intelligence includes key decision criteria such as TCO (total cost of ownership) comparisons and customer satisfaction ratings.

Our research and advisory services cover a range of risk and compliance management topics such as credit risk, market risk, operational risk, GRC, financial crime, liquidity risk, asset and liability management, collateral management, regulatory compliance, risk data aggregation, risk analytics and risk BI.

Our vendor selection services include:

- Buy vs. build decision support.
- Business and functional requirements gathering.
- Identification of suitable risk and compliance implementation partners.
- Review of vendor proposals.
- Assessment of vendor presentations and demonstrations.
- Definition and execution of Proof-of-Concept (PoC) projects.
- Due diligence activities.

For risk technology vendors

Strategy

Chartis can provide specific strategy advice for risk technology vendors and innovators, with a special focus on growth strategy, product direction, go-to-market plans, and more. Some of our specific offerings include:

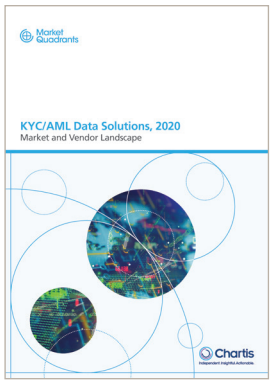
- Market analysis, including market segmentation, market demands, buyer needs, and competitive forces.
- Strategy sessions focused on aligning product and company direction based upon analyst data, research, and market intelligence.
- Advice on go-to-market positioning, messaging, and lead generation.
- Advice on pricing strategy, alliance strategy, and licensing/pricing models.

Thought leadership

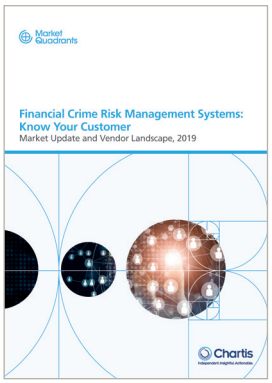
Risk technology vendors can also engage Chartis to provide thought leadership on industry trends in the form of in-person speeches and webinars, as well as custom research and thought-leadership reports. Target audiences and objectives range from internal teams to customer and user conferences. Some recent examples include:

- Participation on a 'Panel of Experts' at a global user conference for a leading Global ERM (Enterprise Risk Management) software vendor.
- Custom research and thought-leadership paper on Basel 3 and implications for risk technology.
- Webinar on Financial Crime Risk Management.
- Internal education of sales team on key regulatory and business trends and engaging C-level decision makers.

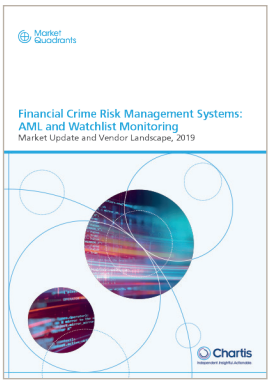
7. Further reading



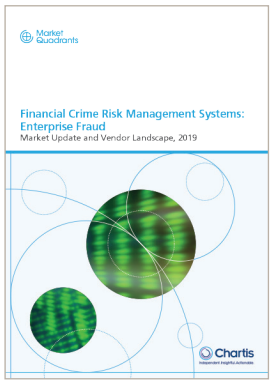
KYC/AML Data Solutions, 2020: Market and Vendor Landscape



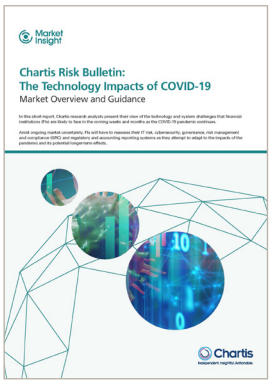
Financial Crime Risk Management Systems: Know Your Customer; Market Update and Vendor Landscape, 2019



Financial Crime Risk Management Systems: AML and Watchlist Monitoring; Market Update and Vendor Landscape, 2019



Financial Crime Risk Management Systems: Enterprise Fraud; Market Update and Vendor Landscape, 2019



Chartis Risk Bulletin: The Technology Impacts of COVID-19

RiskTech100® 2020

For all these reports, see **www.chartis-research.com**