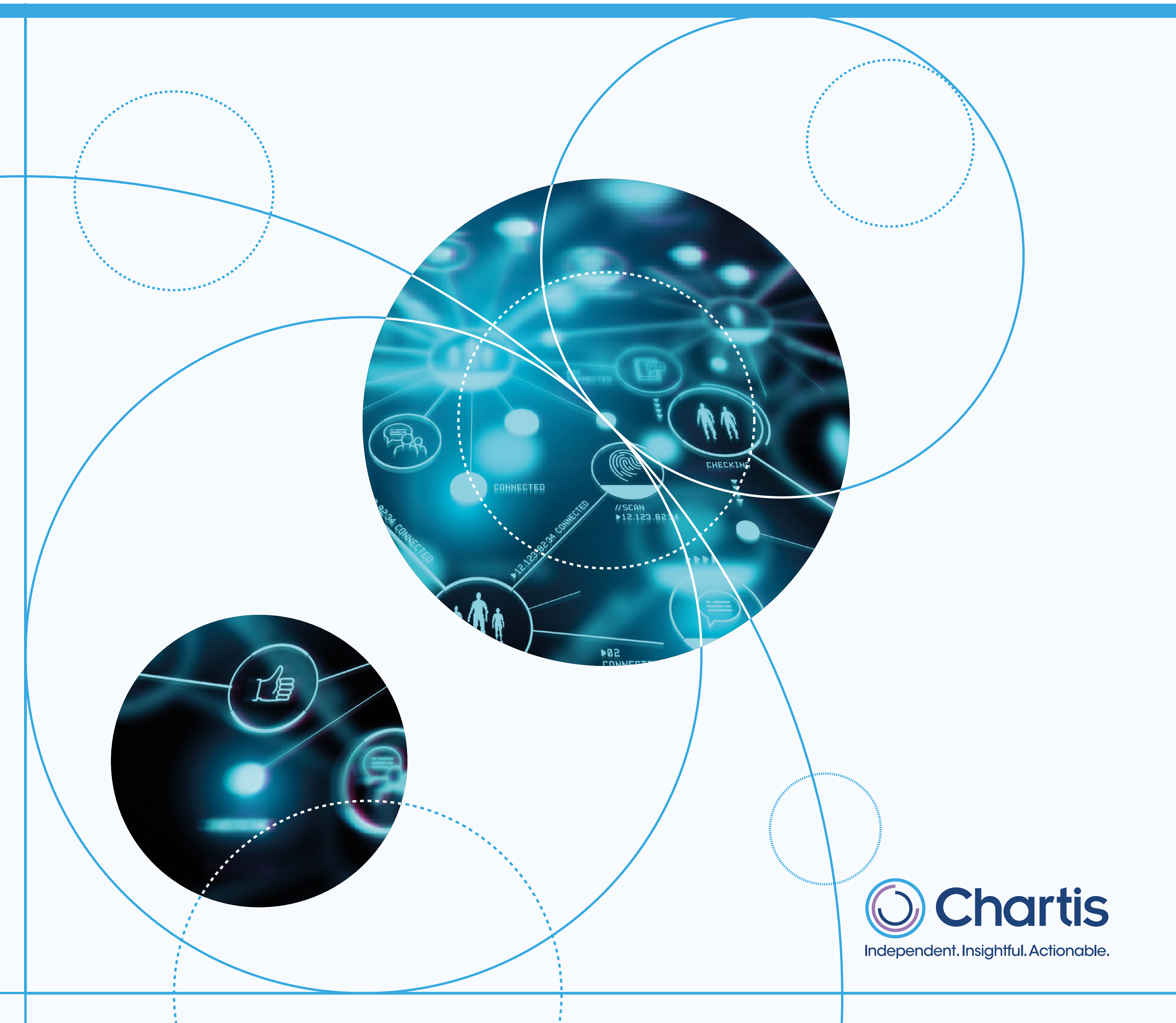
Market Quadrants

Financial Crime Risk Management Systems: Know Your Customer

Market Update 2018



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**.

Please note that the findings, conclusions and recommendations Chartis Research delivers will be based on information gathered in good faith, whose accuracy we cannot guarantee. Chartis Research accepts no liability whatever for actions taken based on any information that may subsequently prove to be incorrect or errors in our analysis. See Chartis 'Terms of Use' on **www.chartis-research.com**.

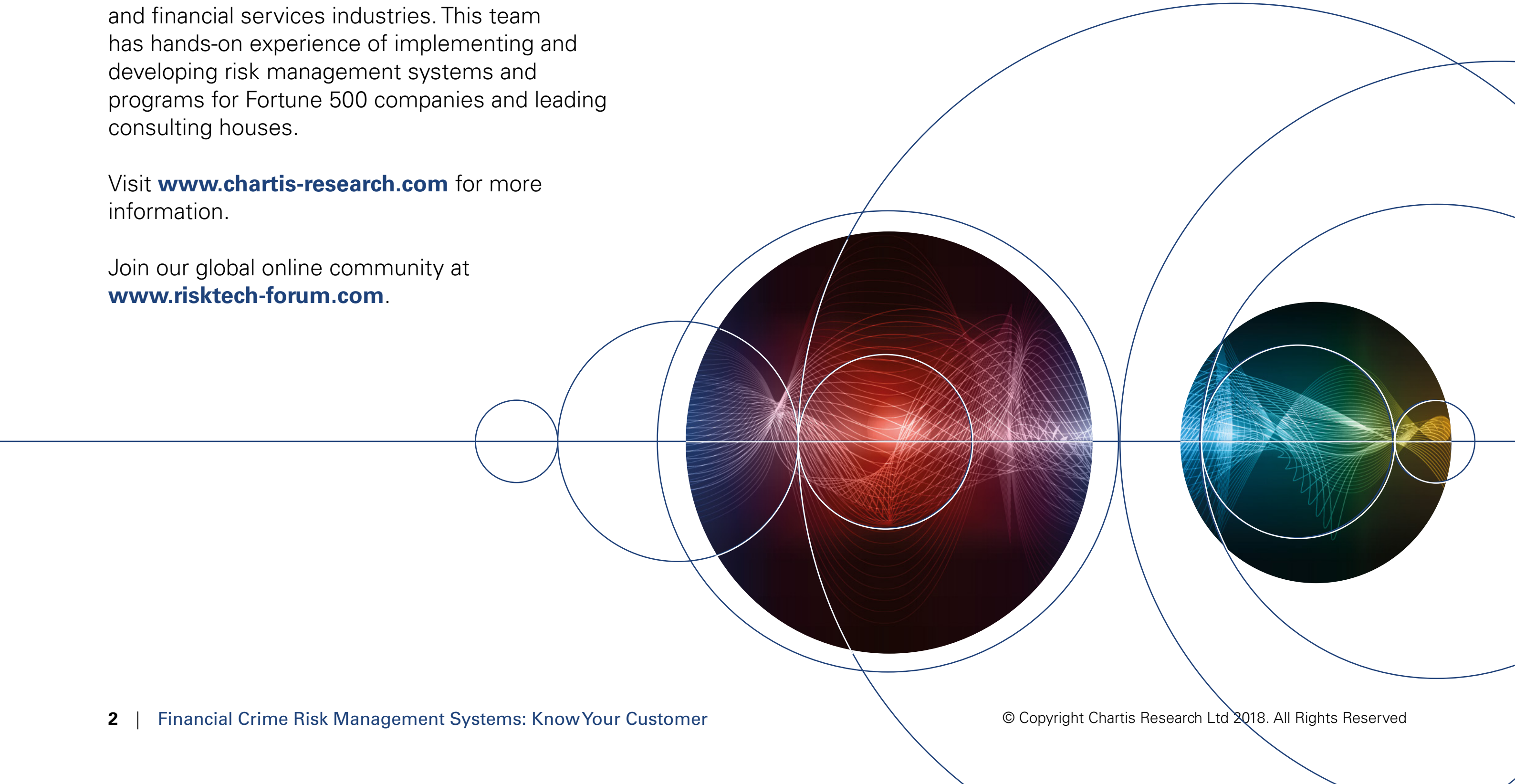


Table of contents

List of figures and tables

1. Executive summary

This report is the first part of Chartis' Financial Crime Risk Management (FCRM) Systems Market Update for 2018. The remaining parts – Enterprise Fraud Solutions, Watchlist/Anti-Money Laundering (AML) Solutions and Trade Surveillance Solutions – will be published later in the year. While previous iterations of our FCRM report included all four elements in one publication, this year we have separated them, to enable us to focus on the individual areas in more detail.

The phrase 'Know Your Customer' (KYC) may sound like a business school management course mantra. In financial services, however, KYC is an important, formalized process, one that has become more complex and workload-intensive in recent years. At its core, KYC is concerned with determining the accurate identity of a customer – a person or a company – and then assessing the risk to a Financial Institution (FI) of conducting business with that entity.

For FIs, the KYC process is now increasingly complicated. To verify a potential customer's identity and examine their risk, KYC analysts must consult a vast, and growing, array of data sources.

Within *retail KYC* – which deals with individuals – these information sources include:

- Lists of government-sanctioned entities.
- Lists of Politically Exposed Persons (PEPs).
- Registries of company ownerships and directorships.

Within *wholesale KYC* – which deals with firms – the information sources include:

- Lists of government-sanctioned entities.
- Lists of state-owned enterprises.
- Company ownership and financial data.
- News coverage of particular firms and entities.

Complicating things further, the exact information that an FI must consult and verify varies greatly across different regulatory jurisdictions. This means that a single, central KYC function may not be enough to deal with different rules around the globe.

With massive datasets to sift through – each with its particular regional quirks and requirements – the numbers of KYC staff FIs employ have risen rapidly. FIs are also becoming more concerned with the risk to their reputation of being accused of helping an entity evade sanctions, even indirectly. This has sharpened their focus on Know Your Third Party (KY3P) and Know Your Customer's Customer (KYCC) – further pushing up the size of their KYC departments.

For years, technology solutions for KYC promised unrealistic results, but FIs are now re-examining how vendors can help them cut costs and improve their operational efficiency. Vendors are responding primarily with technical solutions augmented by large service components. In fact, we estimate that services now comprise a larger proportion of vendor revenue from KYC implementations, although technical advances have continued to provide a strong backbone for vendors' KYC solutions. With this technology/services blend, vendors have focused less on replacing staff outright than on assisting FIs' KYC employees by cutting down on menial tasks.

Vendor innovation is being driven by four key technologies and service models:

- **Workflow automation**. Systems powered by Robotic Process Automation (RPA) and Artificial Intelligence (AI) that reduce much of the repetitive work that KYC analysts engage in (such as document and data retrieval).
- **Profile enrichment**. Third-party data repositories that contain lists of sanctioned entities or details of company ownership structures. These reduce the time that employees spend searching disparate sources for the information they need.
- **Consortia and data sharing**. An organized network of FIs, often anchored around a vendor that provides the requisite infrastructure. These FIs share information, so that customers onboarded at one FI can be assessed more rapidly for another institution.
- **Entity resolution and graph analytics**. Systems to identify customers and prevent duplicate accounts or impersonation. Graph analytics aims to do this using networks to determine identities more precisely and confidently.

These models can apply in different areas of the KYC process, and the vendor landscape is highly differentiated. KYC vendors generally fall into one of the following categories:

- Data providers.
- Data hubs/anchors for consortia.
- Entity resolution specialists.
- Workflow specialists.
- Packaged KYC providers.
- Providers of enterprise financial crime solutions.

Faced with a complex market, FIs must carefully select the KYC components that suit their needs. They must also determine how to implement their chosen system – will they integrate the components themselves, contract an implementation firm to stitch it together for them, or choose an out-of-the-box KYC/financial crime solution? To ensure they make the right choices and meet their objectives, FIs must carefully consider the nuances of their KYC requirements and the offerings available.

Our recommendations for KYC vendors include:

- **Develop services partnerships**. Due to FIs' use of implementation partners, component vendors should ensure they build the links that put them on major consultancies' radar screens when searching for new solutions in their respective KYC systems.
- **Improve systems integration**. In the same vein, vendors should bolster their solutions' capacity to work seamlessly with other KYC components, as well as core banking systems. This will strengthen FIs' KYC workflow and boost their solutions' appeal to FIs and implementation partners.
- **Deepen services offerings**. Work to provide better services – like rules suggestions – within their KYC solution. For example, offer solution extensions that interface with external services such as Dun & Bradstreet for profile enrichment.
- **Offer proof points**. Assure FIs and implementation partners of their solutions' strengths now that systems are able to hit the targets for false positives reductions and onboarding times that previously proved unattainable.

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; it has a sophisticated ranking methodology to explain which solutions would be best for buyers, depending on their implementation strategies.

This report covers the leading providers of KYC solutions: Accuity, Arachnys, BAE Systems, Booz Allen Hamilton, EastNets, Equiniti, Fenergo, FICO, Fiserv, IHS Markit, iMeta, Intellect Design, LexisNexis Risk Solutions, Manipal Group, NICE Actimize, Oracle, Pega, Pitney Bowes, Quantexa, Safe Banking Systems, SAS and Thomson Reuters.

2. Demand-side analysis

KYC is the process by which FIs identify customers and assess the risk they might pose. At its heart, the first step in KYC is a problem of data validation, with two main questions to answer:

- How can an FI ensure that a prospective customer – whether an individual or a firm – is who they say they are?
- Having established the customer's identity, how can they assess the risk – of regulatory infringement or reputational damage – that doing business with that customer presents?

Rigor and speed: two competing requirements

FIs can face severe penalties for accepting a customer that is on a governmental sanctions list. So they must put rigorous systems in place to prevent the onboarding of certain entities – not just those that are clearly off limits, but also those masquerading as other entities in order to appear legitimate. These systems must also incorporate strong audit procedures so that FIs can examine the evidence and documents that led to a customer being accepted or denied.

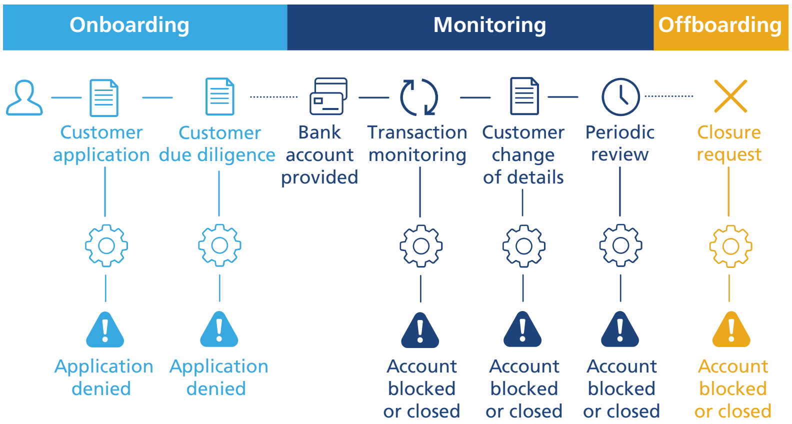
Figure 1 demonstrates the full KYC lifecycle, including *customer monitoring* and *offboarding*. The former is required to ensure that existing customers' accounts are not used – with their knowledge or not – by high-risk entities. The latter ensures that accounts are properly closed, preventing a similar event from occurring after a customer has left the FI.

The level of verification required renders this process highly workload-intensive. In the course of performing KYC checks, FIs must examine documents submitted by customers, government watchlists and external sources to assess a customer's risk. Yet as clients become accustomed to faster and faster delivery of services, and come to expect quick decisions, FIs are being pushed to onboard customers more rapidly. Slow KYC processes can result in lost business as customers look elsewhere.

The type of work a KYC employee must perform varies depending on the type of entity being assessed:

- **Retail** KYC processes look at **individuals**, typically within the insurance or retail banking areas. This involves large volumes of entities – some institutions handle millions of customers – but the complexity of the relationships being analyzed is relatively low. After an individual's identity has been ascertained and verified, the FI must determine whether the risk they present makes them worth doing business with. The FI's policies supply the answer to this question. Because of this, FIs looking for retail KYC systems tend to opt for those with strong workflow and data storage capabilities, to minimize repetitive work and send configurable reports to analysts with pertinent information.
- **Wholesale** KYC processes look at **firms**, typically within corporate banking, investment banking and asset management. In contrast to retail KYC, the volumes involved are low, with customer numbers in the hundreds or thousands for a given institution, but the nature of those customers and their relationships is significantly more complicated. FIs must understand the interrelationships between a firm's subsidiaries and the complexity this creates in their exposure to other risky entities. Wholesale KYC systems thus require stronger entity resolution capabilities and data frameworks that can hold the complex details of these relationships.

Figure 1: KYC process lifecycle



Source: Chartis Research

People power – and cost

In order to perform the requisite checks while at the same time keep up with demands for rapid processing, the wage bills for FIs' KYC functions have ballooned. In addition, the more changes a system incorporates – like adding functionality to assess a person's social media profile or examine a firm's annual reports – the more tailored configuration and training is required to manage the moving parts. Manual – and often menial – tasks form the backbone of today's KYC processes, particularly at smaller FIs with lower budgets.

Beyond the complexity of systems, staff numbers are inflated further by regulatory divergence. Simply put, one centralized KYC function is not enough if regulatory requirements vary wildly across jurisdictions. Instead, FIs often have multiple KYC teams serving different countries or regions, to try and improve workers' efficiency by improving their familiarity with different regulations.

KYC analysts are being tasked with investigating networks beyond the FI's immediate relationships. FIs' growing interest in KY3P processes has also heaped yet more work on their compliance departments, pushing KYC staff counts still higher. FIs want to understand who their customers may be selling goods or services to, or providing finance to – though the bank's counterparty might carry relatively little risk, it may be transacting with sanctioned entities. FIs have become more interested in preventing the possible damage to their reputations implied by having an indirect relationship with an unsavory entity. Greater data availability has enabled FIs to map out these often murky ties. For example, the violation of export controls on military technology – whether perpetrated knowingly or not – carries severe penalties. And if an FI's customer is hit with a large fine, the FI could be at greater risk of providing finance to or relying on deposited funds from that firm, raising the counterparty's credit risk in the process.

A new KYC variable: digital IDs

In emerging markets, the arrival of *digital identities* will alter the KYC onboarding process. Although developed economies have established methods for identifying residents (such as social security numbers in the US), many industrializing nations are only now introducing unique identifiers for their citizens. For FIs in these countries, such changes present both opportunities and challenges.

A unique alphanumeric string for each citizen is a rigorous way to verify an individual's identity, and should resist criminals' attempts to steal that identity. If a person's bank accounts are tied to the same identifier as their state benefits they will be more resistant to allowing others access to it, and will be more careful about disclosing it. The advantages of such a system will be particularly apparent in countries where other signifiers (such as addresses) often differ across the country, making them less useful in resolving customers' identities.

However, adopting a state-run nationwide identity system raises important privacy concerns. Less mature markets may lack institutional frameworks and a culture that values the safeguarding of personal information. If customers are to provide their government-issued identifiers during a KYC process, FIs must protect that data appropriately, and demonstrate this to the customers.

Finally, though the inclusion of digital identifiers will help the entity resolution process, it will add another field for KYC analysts to verify. Many retail customers in emerging markets may deposit or transact infrequently, and the requirement to verify another data source may increase the likelihood that customers will be refused service. FIs must carefully consider how they will adapt their systems to incorporate digital identities – taking advantage of their benefits for customer verification while reducing the proportion of potential customers who may be excluded for entering this new, and possibly unfamiliar, piece of information incorrectly.

Services stepping up

Facing a regulatory mountain of watchlists and business demands for more rapid onboarding, KYC departments threaten to grow into huge hives populated by workers engaged in repetitive drudgery. Consequently, FIs are turning to vendors that can bring staff costs under control and make the way they deal with the growing complexity of KYC investigations more efficient. Notably, rather than raw technology solutions, these offerings typically comprise services combined with systems. Despite attempts to automate the process, the capabilities of past KYC systems have often been exaggerated, and vast reductions in false positives and onboarding times have failed to materialize.

Now, KYC is seen as something vendors can help FIs do well, and those efficiency boosts – albeit reduced – can now be achieved in the form of *solutions* complemented by *services*. We believe that the proportions of expenditure on services and technology have roughly inverted, and that spending on services now comprises the bulk of expenditure on KYC projects. These services range from helping with implementation and tailoring systems to enabling membership of consortia and providing and enriching profile data on request.

Inevitably this will mean that employee numbers will be reduced. But instead of replacing their staff outright, FIs now focus on helping them become more efficient. They are looking more for a robot hand to gather and collate information for humans to review, rather than a magic box that struggles to think on its (artificial) feet.

So what are the implications of these broad trends for the vendor landscape?

3. Supply-side analysis

New techniques and services

To address the challenges FIs now face, vendors are offering new solutions and services that aim to cut FIs' spending by reducing the number of KYC staff they employ. By lowering the number of actions that rely solely on human involvement, these new techniques aim to make KYC processes like onboarding faster and more accurate. Applied correctly they promise to:

- Help FIs ensure that potentially valuable customers are not denied service.
- Prevent the onboarding of those that may appear safe yet hide an unacceptably high level of risk.

Four solution and service models have emerged to tackle the challenges of KYC, which we explore in more detail below, before considering the impacts on the vendor landscape:

- Workflow automation.
- Profile enrichment.
- Consortia and data sharing.
- Entity resolution and graph analytics.

Workflow automation

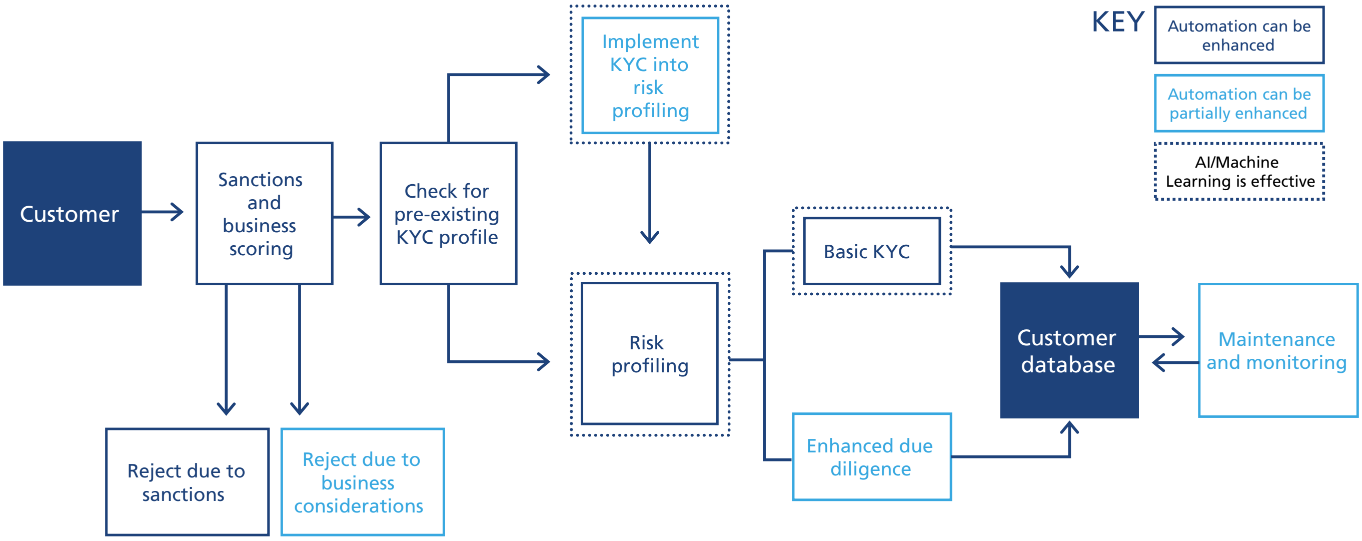
Repetitive due-diligence requirements, like checking a potential customer against sanctions lists, make up much of the workload undertaken by KYC employees. Automating workflow elements can save costs and allow FIs to reallocate employees to more complex tasks such as more intensive investigations and managing higher-value clients.

To automate these components and offer a more streamlined workflow engine, vendors must examine which processes are best suited to automation. The activity to consider should be:

- Consistent, with identical steps performed repeatedly.
- Template-driven, with data being entered into specific fields in a repetitive manner.
- Rules-based.

The actions that fit these criteria rarely cover the entire process that compliance employees perform, so automation should be used to assist their workflow rather than replacing them. Figure 2 shows areas of the KYC workflow that vendors can automate, highlighting those where AI or Machine Learning (ML) can apply.

Figure 2: Automating the KYC onboarding workflow


KEY
Automation can be enhanced
Automation can be partially enhanced
AI/Machine Learning is effective
Customer
Sanctions and business scoring
Check for pre-existing KYC profile
Implement KYC into risk profiling
Risk profiling
Basic KYC
Enhanced due diligence
Customer database
Maintenance and monitoring
Reject due to sanctions
Reject due to business considerations

Source: Chartis Research

In order to successfully automate elements of the KYC workflow, FIs must choose from an often-bewildering array of technologies, each with their own promises of benefits.

The three key technologies that will best enhance KYC workflow automation are:

- **Robotics**. Using methods such as screen-scraping, macros and recording functionality, RPA can capture and replicate repetitive work. Although FIs can use RPA systems without generally reconfiguring their core software, they must integrate these systems effectively with the overall application to ensure their accuracy.

- **Integration**. By constructing rigorously defined Application Programming Interfaces (APIs), FIs can enable cohesive, standardized data transfer between elements of the process. APIs can facilitate event-driven workflow, automatically triggering a process according to the occurrence or outcome of an event.

- **AI**. This is often considered a natural extension of automation: FIs can apply AI tools to change the nature of the automated process. ML techniques, for example, can be used to transform ‘static’ automation into ‘dynamic’ automation, which responds to inputs without human intervention and/or offers more appropriate outcomes, recommendations and analysis.

Among vendors, workflow specialists, packaged KYC providers and enterprise financial crime providers are leading the pack in terms of automation capabilities, which include RPA and the capability to create ‘intelligent’ rules. This involves using pattern analysis (potentially ML or other capabilities) on pre-existing rules to determine new ones (such as time of onboarding, location or device identity). These rules may not be part of the traditional onboarding process but can be reviewed and tested by an analyst to see if they provide increased efficacy (see Figure 3).

Profile enrichment

For FIs, third-party data has proved extremely useful in cutting the amount of time employees must spend collating and reconciling information. The most useful data sources for FIs include:

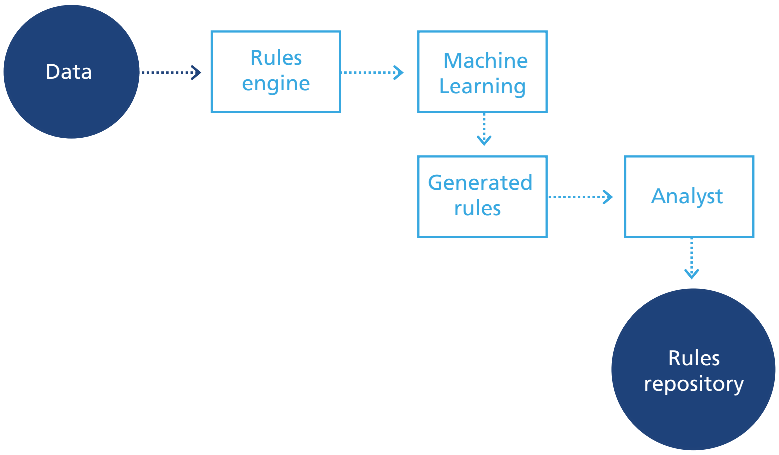
- Lists of sanctioned entities.

- Lists of state-owned enterprises.

- Lists of PEPs.

- Repositories of Ultimate Beneficial Ownership (UBO) data.

Figure 3: Intelligent rules generation



Source: Chartis Research

Access to sanctions watchlists is of vital importance to FIs in complying with the law. The other three data sources help inform and augment FIs’ risk scoring for each customer according to each FI’s internal risk-weighting policies. For instance, knowing that an individual is a PEP from a country regarded as corrupt is useful in assessing their risk compared to that of a shop owner.

Consortia and data sharing

Consortia, in which banks share information on customers, solve two major problems:

- **Divergent data requests**. The documents and other information that FIs request for KYC processes often differ, both within and across institutions. If an FI has the wrong documents it can be fined for non-compliance, while the inconvenience or confusion caused by inconsistent document requests can frustrate customers, reducing the efficiency of onboarding.

- **Lack of up-to-date information on entities**. FIs find it difficult to ascertain if or how a legal entity’s circumstances have changed – if an individual changes address, for example, or a firm’s ownership changes. To remain compliant, FIs must expend resources chasing down current information on customers.

Consortia can alleviate these issues by encouraging FIs to share their customer data. A consortium is often provided as a service by a vendor that 'anchors' a group of FIs and maintains the master dataset. By providing a single source of truth in this way they can help FIs reduce inconsistent document requests and maintain current information on customers.

Data sharing is most successful in regions with a large number of smaller institutions that may not have the resources to manage KYC effectively on their own. In addition, institutions within a successful consortium should be subject to the same or similar regulation. For this reason, there may be issues with consortia around data privacy. With regard to the General Data Protection Regulation (GDPR), for example, although customer data may be secure within banks, pooling Europeans' data may present difficulties, particularly if non-banks – which have traditionally had weaker data controls – are involved.

Entity resolution and graph analytics

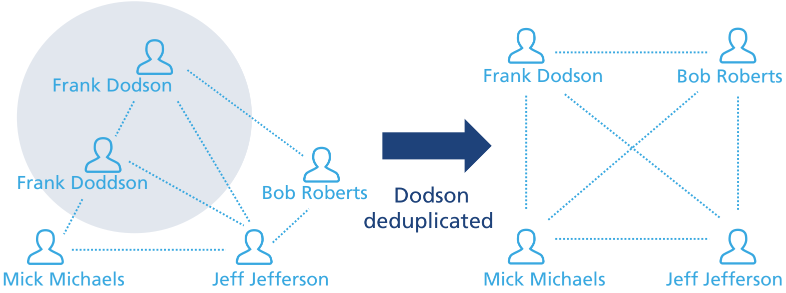
The process of *entity resolution* requires four capabilities:

- **Deduplication**. Eliminating extraneous records that relate to the same entity within a dataset.
- **Record linkage**. Matching records from one deduplicated data store with another.
- **Referencing**. Matching noisy or damaged records to clean reference tables (e.g., matching 'Fr-nk D-ds—' to a pre-existing reference 'Frank Dodson').
- **'Canonicalization'**. Converting data into a standardized or 'canonical' form.

Traditional relational databases can struggle with these steps, because of the huge volume of relational data about customers, which produces large, unwieldy datasets and slow processing times.

Graph analytics can be an efficient way to resolve a customer's identity. It represents information as nodes and relationships in a network, so KYC analysts can more accurately assess a number of the capabilities listed above. Deduplication, for example, can be performed by measuring the 'distance' between entities to determine whether tightly clustered entities are, in fact, the same thing. Links between records and references can be considered as 'edges' between entities. By assessing how tightly grouped a given dataset is, for example, KYC analysts can judge the likelihood that a given individual is indeed the one in question (see Figure 4).

Figure 4: Graph analytics for entity resolution and deduplication



Source: Chartis Research

Again, traditional relational databases struggle here. They store relationships between entities as one-to-one connections, and to preserve the many-to-many relationships necessary for graph analytics they require additional customization (such as additional tables that keep record connections). This relatively inelegant solution can result in slow processing times if faced with the huge volumes of data describing the customer base of a larger retail bank, for example, or the more complex relationships between customers of wholesale institutions.

The vendor landscape – choose carefully

If deployed correctly, these new solutions and services for KYC promise big benefits. FIs must choose carefully when deploying new KYC systems and processes, because the vendor landscape is highly differentiated, with KYC suppliers falling into several categories (see Table 1).

Table 1: KYC solution providers – a differentiated group

Category of provider	Comments
Data providers	• Supply external data on sanctioned or high-risk entities. • Typically specialize in a service that offers access to updated lists of sanctioned entities and state-owned enterprises. • May also maintain proprietary repositories of data on company ownership, which enables ultimate beneficial owners to be identified, as required by regulations such as the Financial Crimes Enforcement Network (FinCEN) Final Rule and the EU's Fourth Anti-Money Laundering Directive (4AMLD). • By collating data required for KYC, these vendors reduce the manual work needed to gather information and allow FIs to focus on risk scoring and customer management. • The strongest vendors typically provide access to information on the largest number of entities, and offer a method by which FIs can smoothly ingest this data into their KYC processes.
Data hubs/consortium anchors	• Like data providers, these vendors offer access to a database of entities. • Information is often provided by the FIs themselves, which pool entity information for retail or wholesale business lines. • Due to network effects, whereby having more members vastly increases the benefits of membership, some of these consortia have garnered enough market share to become key elements of the retail or wholesale KYC process for a large number of institutions.
Entity resolution specialists	• Provide the systems that underpin the 'who's who' of KYC, by reconciling multiple sets of information to determine an entity's true identity. • The performance of the entity resolution systems is defined by the speed at which they can identify the probability of a match, the accuracy of that result, and the volume of entities handled. • Vendors with the best entity resolution solutions go beyond mere pair-wise comparisons – checking for similar addresses listed for notionally distinct individuals, say – to using relational data to analyze the likelihood that a set of data matches a given entity.
Workflow specialists	• Offer a workflow engine and a set of rules for assessing customer risk. • Workflow engines should be flexible and reduce the time staff spend on 'busywork' (such as retrieving documents). • The strongest vendors have capabilities that monitor workflows for repetitive actions and offer rule-set suggestions based on users' behavior.
Packaged KYC providers	• Provide a full KYC system that incorporates workflow and entity resolution, as well as streams for ingesting external data. • Strong vendors offer easy configuration of rule sets, as well as workflow capabilities and data storage frameworks.

Category of provider	Comments
Enterprise financial crime providers	• Offer complete or near-complete KYC functionality as part of a larger financial crime solution that may cover AML and fraud detection. • The emphasis on KYC is often less in these systems because fines for violating AML regulations dwarf those in KYC, though AML is much less process-intensive. • By providing KYC and AML systems in one package, however, vendors can use transaction monitoring data to inform entity resolution and risk scoring in KYC processes.

Source: Chartis Research

In addition to a varied supplier landscape, FIs face multiple choices in the way they implement a KYC system:

- **In-house build**, which may integrate components from different vendors (assuming it is not done entirely in-house). In this case an FI selects the components and suppliers that suit its requirements – an entity resolution system from one vendor, say, and a workflow engine from another – before integrating them into a custom KYC system. This option is best for specialized institutions that may require a certain entity data model or a peculiar workflow pattern.

- **Assisted implementation**, using components packaged by an implementation partner. In this case an FI selects an implementation firm that offers a 'set menu' of KYC components best suited to its needs, or which advises on systems the FI can integrate 'a la carte'.

- **Enterprise financial crime solutions** with KYC as a component. Here an FI selects a vendor to supply a full financial crime suite that includes KYC. This is especially useful if the institution already has a relationship with the vendor and uses its platform or complementary solutions.

Because of this, the RiskTech Quadrant® for KYC solutions should not be the only input an FI uses when considering an offering. No vendors provide market-leading capabilities for every area of the KYC process, so FIs should consider their strategy before selecting a vendor, referring to the vendor capabilities table in detail. If they have a large backlog of unresolved onboarding data, for example, it may be wise to invest in an entity resolution specialist. If they wish to establish the 'building blocks' of a system that will be expanded in future, they may wish to start with a workflow specialist, or a well-rounded enterprise financial crime risk management vendor.

RiskTech Quadrant® for KYC solutions, 2018

Figure 5 describes Chartis' view of the vendor landscape for KYC solutions. The RiskTech Quadrant® is a proprietary methodology developed specifically for the risk technology marketplace. It takes into account the product and technology capabilities of vendors, as well as their organizational capabilities.

Table 2 rates the specific capabilities of the vendors.

Appendix A sets out the generic methodology and criteria used for the RiskTech Quadrant®. Specifically, we have considered the following criteria as particularly important:

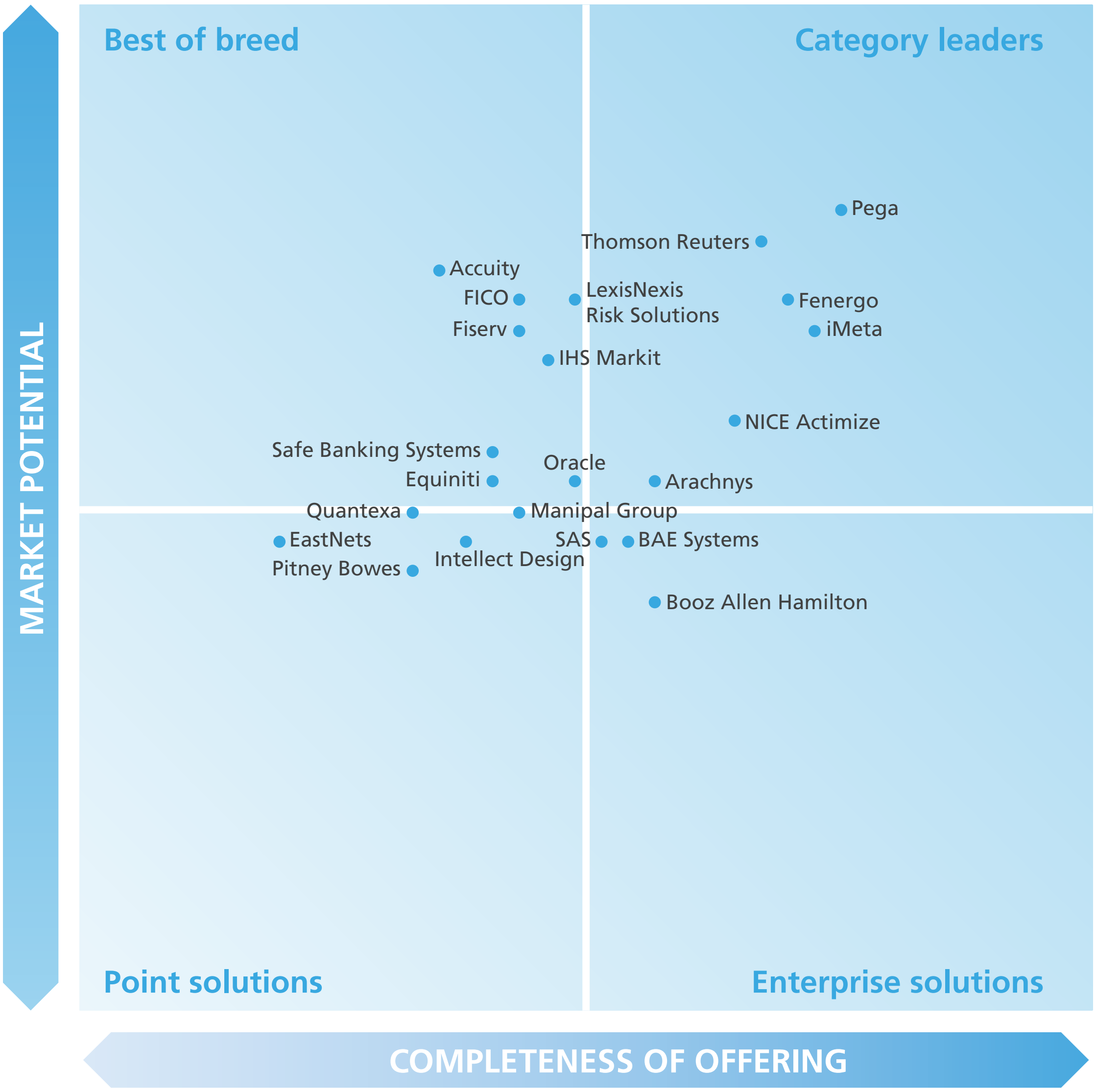
Completeness of offering:

- Reporting and dashboarding.
- KYC risk scores.
- Customer profile enrichment with additional data.
- Customer lifecycle management.
- Entity resolution.
- Customer onboarding.
- Workflow engine.

Market potential:

- Customer satisfaction.
- Market penetration.
- Growth strategy.
- Financials.

Figure 5: Chartis RiskTech Quadrant® for KYC solutions, 2018



Source: Chartis Research

Table 2: Vendor capabilities table for KYC solutions, 2018

	Entity resolution	Reporting and dashboarding	KYC risk scores	Customer profile enrichment with additional data	Customer lifecycle management	Customer onboarding	Workflow engine
Accuity	*	**	**	***	*	**	*
Arachnys	**	**	**	**	*	***	**
BAE Systems	*	**	**	**	**	**	***
Booz Allen Hamilton	**	**	**	**	*	**	***
EastNets	*	*	*	*	**	*	**
Equiniti	*	***	***	***	*	*	*
Fenergo	***	**	**	**	***	**	**
FICO	**	**	**	**	*	**	**
Fiserv	**	***	*	***	*	*	**
IHS Markit	*	***	**	***	*	**	*
iMeta	***	***	***	**	***	**	**
Intellect Design	**	*	**	*	*	**	**
LexisNexis Risk Solutions	*	***	**	***	*	*	**
Manipal Group	*	**	**	*	**	**	**
NICE Actimize	**	**	**	**	**	***	***
Oracle	**	*	*	***	**	**	**
Pega	**	*	***	**	***	***	***
Pitney Bowes	***	**	*	*	*	*	*
Quantexa	***	**	*	*	*	*	*
Safe Banking Systems	***	**	*	*	*	**	*
SAS	**	**	**	**	**	**	**
Thomson Reuters	**	***	***	***	*	***	*

*Key: *** = Core strength/advanced capabilities; ** = Meets industry requirements; * = Partial coverage/component capability.*
Source: Chartis Research

Advice for vendors

To successfully bolster their KYC offerings and gain clients, vendors should capitalize on their existing strengths. Many of those that Chartis researched disavowed any mission creep or extending too far, stating that they would not be branching out into areas of KYC in which they had no expertise. With this in mind, we believe that an ecosystem in which many vendors provide individual modules for the KYC process will persist. Although large 'one-stop shops' for KYC and enterprise financial crime risk management solutions will retain market share, most of those vendors with whom we spoke had partnerships with smaller suppliers that augmented their offering.

Moving forward, our advice to KYC vendors is to:

- **Develop services partnerships**. This means building relationships with implementation partners – firms with experience in implementing KYC and financial crime systems often prefer to offer a set of systems that they are experienced in delivering to clients. Although these firms – frequently large consultancies – may offer bespoke implementations, many prefer to provide a comprehensive package for which they have built the requisite connective tissue between components they are familiar with (for example, entity resolution from one vendor and workflow from another). Once an implementation partner has built its KYC/financial crime 'set menu' around a vendor's solution, that vendor will enjoy a more secure revenue stream as its solution proves hard to displace.

- **Improve systems integration**. Vendors should offer open APIs to integrate their solution more effectively with other KYC systems. This approach can help to promote event-based triggers by allowing other systems to raise flags within the KYC module, assisting workflow. For example, if a customer transfers a large sum to a high-risk entity, this can throw a warning within the KYC suite that requires manual inspection. It would also enable the vendor's solutions to interact with systems such as the FI's core banking platform, allowing it to automatically close or suspend accounts and similarly improve KYC workflow. Doing this will make the vendor's offering more appealing to a services partner, because the integrator can easily assemble a full KYC suite by stitching together well-defined components rather than by mashing together conflicting parts.

- **Deepen their services offerings**. Suppliers should augment their solutions by offering access to external services directly from an interface within the KYC application. Charging by request for profile enrichment queries to proprietary data sources like Dun & Bradstreet presents a promising avenue for workflow providers, for example – rather than requiring a full subscription, an institution can pay its KYC vendor for the use of the service only as required. These advantages will also help to prevent a competitor displacing the vendor. More fully fledged services, meanwhile, provide other avenues for revenue and deeper client relationships. Vendors could offer other financial crime services (such as transaction monitoring), or customer lifecycle management services (like product marketing and accounting).

- **Offer proof points**. By offering these for their systems, vendors can assure FIs of their systems' performance. These proof points could include:

- Benchmarking.

- Case studies.

- Model validation.[1]

Conclusion

As sanctions lists grow and due diligence requirements proliferate, FIs face a possible future of flabby KYC functions poorly configured to meet intensifying customer demands for rapid onboarding. There is another way, however – accepting that technology cannot do it all and is instead better employed to help staff work more efficiently. With the right model in place, technology solutions can help flesh and blood investigators to focus on more high-value work, delivering better outcomes for all.

[1] *Please refer to Chartis' forthcoming Model Validation report for more on this.*

4. Appendix A: 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's 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's 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's opinion. Risk technology vendors cannot purchase or influence positive exposure. Chartis adheres to the highest standards of governance, independence, and ethics.

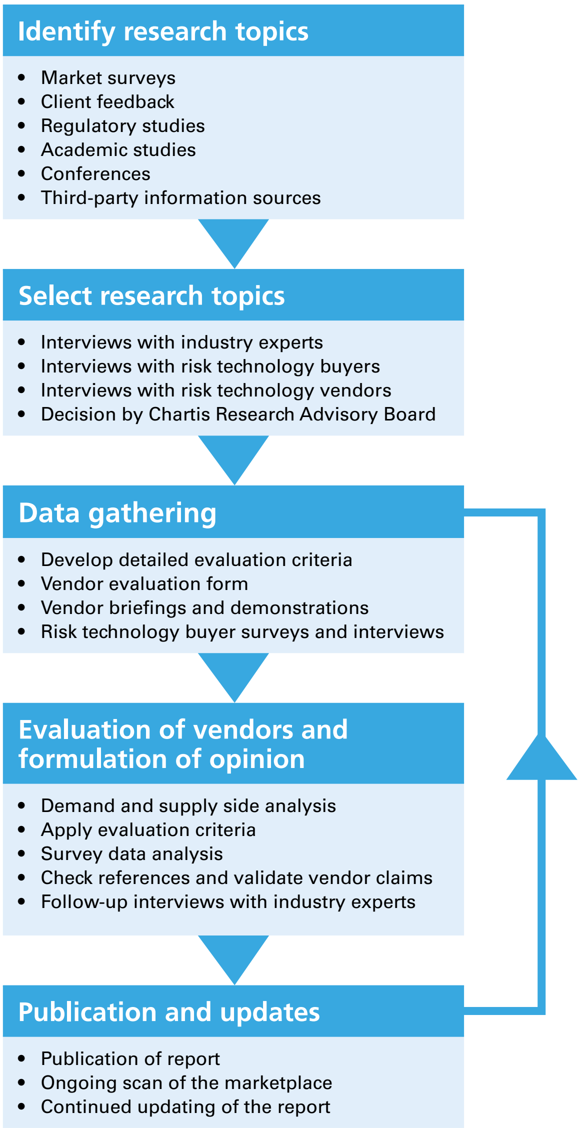
Inclusion in the RiskTech Quadrant®

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 6 below describes the research process.

Figure 6: RiskTech Quadrant® research process



Identify research topics

- Market surveys
- Client feedback
- Regulatory studies
- Academic studies
- Conferences
- Third-party information sources

Select research topics

- Interviews with industry experts
- Interviews with risk technology buyers
- Interviews with risk technology vendors
- Decision by Chartis Research Advisory Board

Data gathering

- Develop detailed evaluation criteria
- Vendor evaluation form
- Vendor briefings and demonstrations
- Risk technology buyer surveys and interviews

Evaluation of vendors and formulation of opinion

- Demand and supply side analysis
- Apply evaluation criteria
- Survey data analysis
- Check references and validate vendor claims
- Follow-up interviews with industry experts

Publication and updates

- Publication of report
- Ongoing scan of the marketplace
- Continued updating of the report

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's 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.

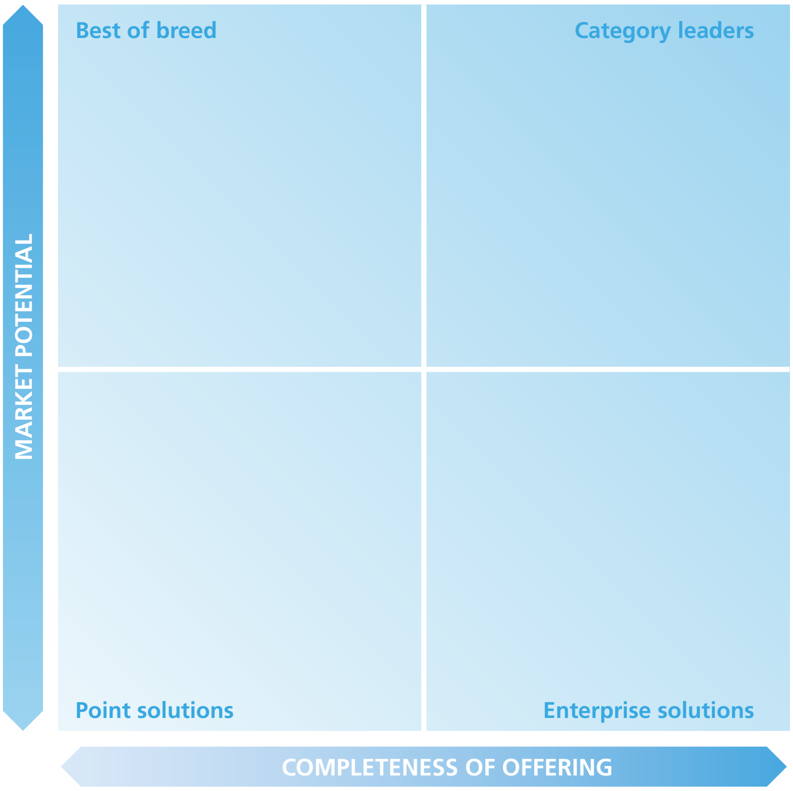
Evaluation criteria

The RiskTech Quadrant® (see Figure 7) evaluates vendors on two key dimensions:

1. Completeness of offering

2. Market potential

Figure 7: RiskTech Quadrant®



Source: Chartis Research

The generic evaluation criteria for each dimension are set out below. In addition to these generic criteria, Chartis utilizes domain-specific criteria relevant to each individual risk, which are available on request. This ensures total transparency in our methodology and allows 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

- **Market penetration.** Both volume (i.e. number of customers) and value (i.e. average deal size) are considered important. Also, rates of growth relative to sector growth rates are evaluated.

- **Brand.** Brand awareness, reputation, and the ability to leverage current market position to expand horizontally (with new offerings) or vertically (into new sectors) are evaluated.

- **Momentum.** Performance over the previous 12 months is evaluated, including financial performance, new product releases, quantity and quality of contract wins, and market expansion moves.

- **Innovation.** New ideas, functionality, and technologies to solve specific risk management problems are evaluated. Developing new products is only the first step in generating success. Speed to market, positioning, and translation into incremental revenues are critical success factors for exploitation of the new product. Chartis also evaluates business model or organizational innovation (i.e. not just product innovation).

- **Customer satisfaction.** Feedback from customers 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) is evaluated.

- **Sales execution.** The size and quality of sales force, sales distribution channels, global presence, focus on risk management, messaging, and positioning are all important factors.

- **Implementation and support.** 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.

- **Thought-leadership.** Business insight and understanding, new thinking, formulation and execution of best practices, and intellectual rigor are considered important by end users.

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

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.

5. How to use research and services from Chartis

In addition to our flagship industry reports, Chartis also 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

6. Further reading

RiskTech 100® 2018

Research partner

Media partner

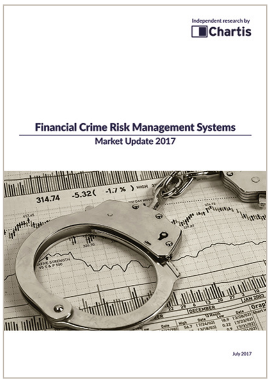
EY Building a better working world

RiskTech FORUM SPOTLIGHT ON RISK TECHNOLOGY

October 2017

Independent research by Chartis

RiskTech100® 2018



Independent research by Chartis

Financial Crime Risk Management Systems

Market Update 2017

July 2017

Financial Crime Risk Management Systems – Market Update 2017

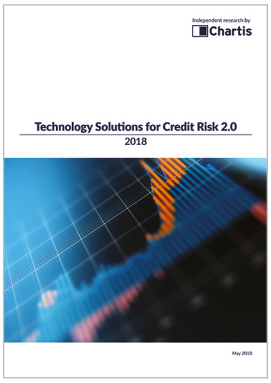
Independent research by Chartis

Front Office Risk Management Technology

2018

June 2018

Front Office Risk Management Technology 2018



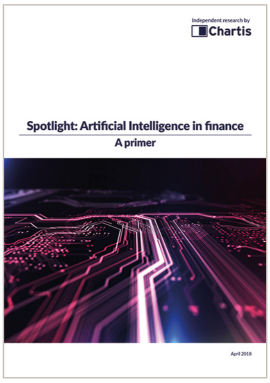
Independent research by Chartis

Technology Solutions for Credit Risk 2.0

2018

May 2018

Technology Solutions for Credit Risk 2.0, 2018



Independent research by Chartis

Spotlight: Artificial Intelligence in finance

A primer

April 2018

Spotlight on Artificial Intelligence in finance – a primer

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