Market Quadrants

KYC Solutions, 2022

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:

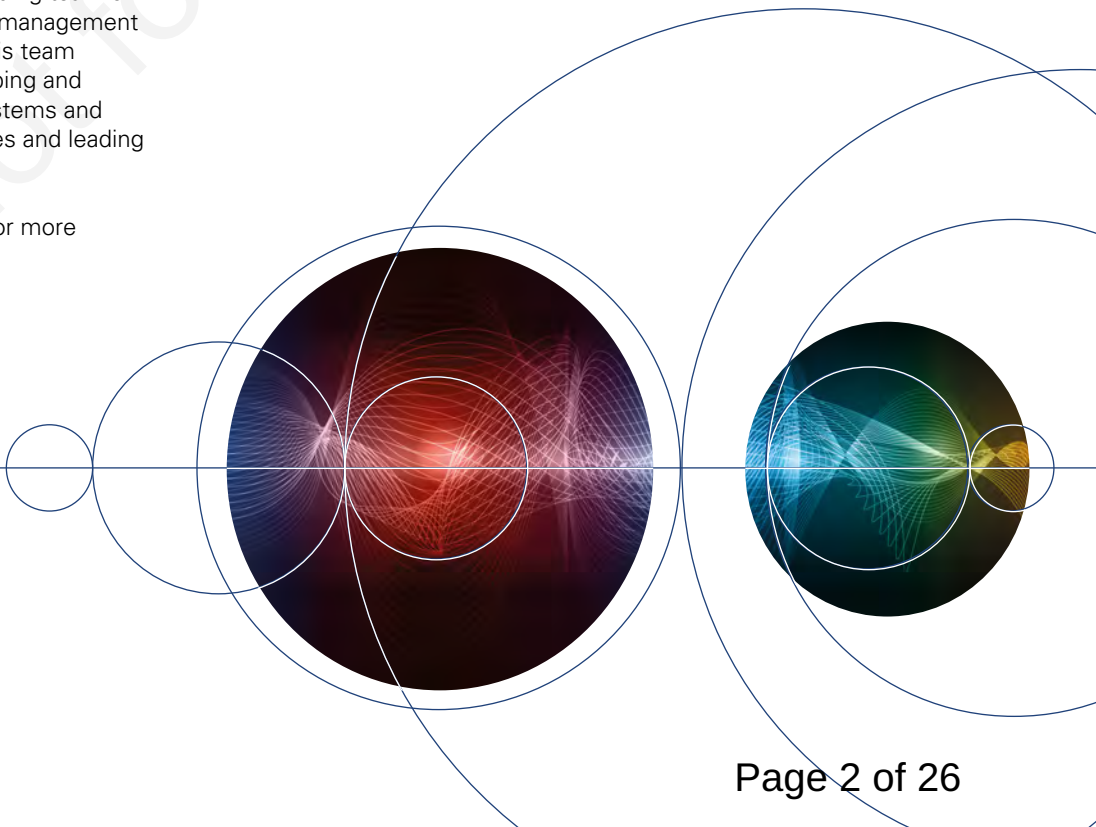
- Credit risk.
- Operational risk and governance, risk management and compliance (GRC).
- Market risk.
- Asset and liability management (ALM) and liquidity risk.
- Energy and commodity trading risk.
- Financial crime, including trader surveillance, anti-fraud and anti-money laundering.
- Cyber risk management.
- Insurance risk.
- Regulatory requirements.
- Wealth advisory.
- Asset management.

Chartis focuses on risk and compliance technology, giving 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 developing and implementing risk management systems and programs for Fortune 500 companies and leading consulting firms.

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

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



05 OCT 2022

Market Quadrants Report

Authors
Phil Mackenzie and Ahmad Kataf

Jump to: **Market update** | **Vendor landscape** | **Chartis RiskTech Quadrant® and tables** | **Methodology**

Executive summary

The macro themes in the Know Your Customer (KYC) solutions market in 2022 are cost saving and efficiency, and include the following sub-themes:

- **Automation**. Having automated relatively simple, repetitive tasks, financial institutions are now tackling more complex processes, including customer due diligence, transaction monitoring and remediation processes. This has led to a stronger focus on flexible workflow capabilities and different automation techniques, including no-code/low-code approaches, rules definition and robotic process automation (RPA).
- **Greater use of artificial intelligence (AI)**. Regulators have become more relaxed about the use of advanced AI and statistics within KYC processes, and have even actively encouraged it through forums and sandboxing events, where regulators can see how well technological solutions work in a live setting. Alongside this, however, institutions are considering more significant use of model risk and benchmarking methods to ensure that AI techniques operate within a contained and comprehensible framework.
- **More ways of testing KYC**. Along with statistical benchmarking, financial institutions are considering a greater variety of ways to quantify the success (or failure) of their compliance processes in. False positives have been a significant metric within the KYC process for years, but institutions are now thinking about quantifying their level of compliance in terms of productivity and time. In addition, online-only 'neobanks' and new types of financial institution are looking at onboarding time and customer experience as differentiators. The numbers of false negatives for these institutions are often more significant.
- **Services vs. technology**. The line between service and technology firms in the KYC space continues to blur. More service firms are entering the technology

marketplace, and technology vendors are continuing to build out their service offerings.

- **Cloud**. The blurring of the line between services and technology has been enabled in part by the growing adoption of cloud technology. Lightweight, containerized solutions can be deployed quickly, and their decentralized nature means they can be accessed by services outside the institution's physical perimeter.

Other notable themes in the market include:

- **Geographical variation** within KYC processes, as institutions must increasingly account for both global and regional regulations, particularly around sanctions.
- **Growing use of more sophisticated methods** for quantifying counterparties, including Know Your Business and Know Your Customer's Customer.

Technology trends in the vendor landscape include the continued prevalence of the cloud and application programming interfaces (APIs) in solution offerings, diversified workflow strategies, and the focus of some vendors on dedicated identity verification (IDV) solutions.

This report uses Chartis' RiskTech Quadrant® to explain the structure of the market. The RiskTech Quadrant® employs 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 – rather, it has a sophisticated ranking methodology to explain which solutions would be most suitable for buyers, depending on their implementation strategies.

This report covers the following providers of KYC solutions: Alloy, AML Partners, Appian, BasisTech, ComplyAdvantage, Diligent, Eastnets, Encompass, Fenergo, FIS, Fiserv, iMeta, KYC Portal, LexisNexis Risk Solutions, Manipal Group, NetReveal, NICE Actimize, Oracle, Pega, PwC, Quantexa, RiskScreen, S&P Global, SAS, Shufti Pro, Sigma Ratings, Silent Eight, smartKYC, SymphonyAI Sensa, Veriff, Vneuron and Zoloz.

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 responded to our requests for briefings, and some declined to participate in our research.

Jump to top

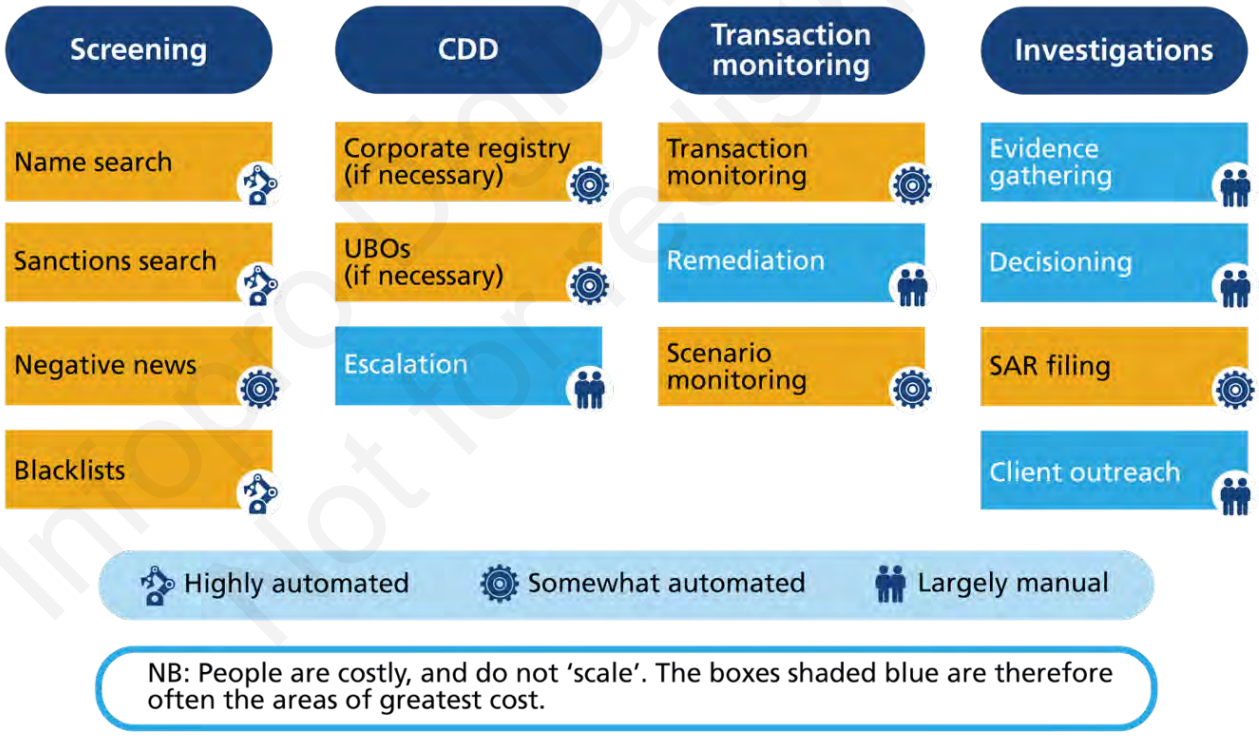
Market update

Key themes for 2022

Efficiency: more automation in the KYC process

Greater automation of the KYC and onboarding process continues across financial institutions, and remains perhaps the primary driver of solution implementations within the KYC space. In the quest for greater productivity, faster onboarding and more efficient use of their staff, financial institutions are considering the use of advanced analytics and enhanced workflow capabilities. However, the level of automation in institutions remains uneven (see Figure 1).

Figure 1: Degree of automation in the KYC process



Source: Chartis Research

Degrees of automation are driven mainly by the simplicity of the action being automated and by the need for responsibility to be assigned to it. As a result, investigations and remediations tend to be relatively unautomated, as human decision-making is a key requirement in the process.

Firms have made significant investments in exploring how to automate these areas. Data analytics, for example, can be used to identify high-risk customers and transactions automatically. This can be done by analyzing customer data that includes account history, demographics and patterns of transactions.

The remediation process can be addressed via flexible workflows and RPA used to automate task assignments and monitoring of progress. Document management processing can also be used to store and retrieve remediation data.

AI: key developments

More encouragement from regulators

In response to more demanding compliance requirements, regulators have started to relax their attitude toward the use of advanced statistics by financial institutions to relieve their compliance burden. This has been helped by a general increase in the adoption of these techniques in the wider technology market.

In October 2019, the Financial Crimes Enforcement Network (FinCEN) issued guidance on the application of AI in anti-money laundering (AML) and combating the financing of terrorism (CFT) compliance. The guidance is intended to help financial institutions understand how FinCEN regulations apply to the use of AI in their compliance programs, and to encourage the development and adoption of innovative technologies to combat financial crime.

The guidance notes that financial institutions are turning increasingly to AI to supplement their conventional AML/CFT compliance efforts. AI can help firms identify and assess risk, detect and investigate suspicious activity, and comply with regulations more effectively. However, the guidance also notes that the use of AI in compliance programs raises a number of potential risks. These include the possibility of bias and errors in decision-making, the need for adequate data to train and test AI models, and the potential for AI-derived information to be misused.

To mitigate these risks, FinCEN's guidance recommends that financial institutions take a risk-based approach to the use of AI in their compliance programs. Firms should use AI-based solutions only if they have a clear understanding of the risks and benefits involved, and should have adequate controls in place to address those risks. In particular, they should ensure that their AI models are trained and tested on high-quality data, have mechanisms in place to monitor and assess the

performance of AI models, and have procedures for addressing errors and biases.

The guidance also stresses the importance of transparency and communication in the use of AI in compliance programs. Financial institutions should be transparent with regulators about their use of AI, and should ensure that their employees and customers understand how AI is being used in compliance programs. Firms should also have policies and procedures in place to ensure the safe and secure handling of AI-derived information.

Such recent events as the **FinCEN Digital Identity Tech Sprint** have enabled institutions to examine how the implementation of technology to reduce fraud, money laundering and terrorist financing can be handled in a live environment.

Model validation and benchmarking now more significant

The growth of AI and advanced statistical techniques has been followed by a corresponding growth in the validation processes that surround them. Model risk is the potential for financial losses caused by errors in the models used for decision-making. In the context of sanctions screening and the KYC process, model risk can arise from inaccuracies in the data used to train the model, incorrect assumptions about the relationships between the data variables, or errors in the model's coding.

The use of machine learning (ML) algorithms for sanctions screening could reduce model risk by automating the feature-selection and model-tuning processes. However, ML models are also susceptible to data-quality issues and overfitting, whereby they can become overly responsive to noise in the data or random changes.

In order to mitigate model risk, it is important that firms use a robust dataset for training and validation, and that they monitor the performance of the model on an ongoing basis. It is also important to have a clear understanding of the limitations of the model and the assumptions made during its development. More specifically, there has been a heightened focus on scalable testing and validity/parameter analysis, which assess the sensitivity of a model to changes in its parameters.

As such, within the analytics space, there has been a move toward vendors with advanced statistical capabilities and a full set of validation and testing tools for these capabilities, including sandboxing and simulation testing.

Efficiency: the growing importance of alternative metrics

False positives are no longer the principal metric used to measure the efficiency of KYC solutions in the onboarding process. Instead, firms are increasingly focusing on productivity metrics, including time spent on the onboarding process, productivity gained from other areas in the business, and so on.

Most onboarding processes tend to have high numbers of false positives: a solution flags an individual or entity as being high-risk, but further investigation determines it to be low-risk. This scenario is a natural outcome of the near-zero risk appetite that most major financial institutions have for sanctions and onboarding risk. By ensuring that their risk systems are as sensitive as possible, they can try to prevent sanctioned entities from passing through their onboarding screen.

However, more firms are now looking at the quantification of false negatives as part of their onboarding solutions and strategies. False negatives occur when a screening system deems an entity to be safe, but closer examination reveals it to be a risk. False negatives have seldom been discussed within the compliance space until recently, largely because they are difficult to detect. Once an institution has marked an entity as safe, that entity is typically not identified as a risk until some external factor reveals it as such. This, combined with institutions' low risk appetite, has led to the view that false negatives are a relatively insignificant metric.

Newer financial institutions (such as neobanks and crypto firms), however, have been moving increasingly toward the quantification of false negatives. These institutions often have greater appetites for risk, and prioritize the quick and effective onboarding of customers. This has pushed their risk profiles higher, making them more inclined to focus on ensuring that individuals are not held up in their onboarding process.

Outsourcing and the cloud

There are several benefits in using cloud-based services for KYC compliance. Firstly, they allow financial institutions to outsource the storage and management of customer data to a third-party provider. This frees up internal resources that can be better used for other tasks. Secondly, cloud-based services can be more cost-effective than on-premises solutions. This is because they require no upfront investment in hardware or software, and can be scaled up or down as needed.

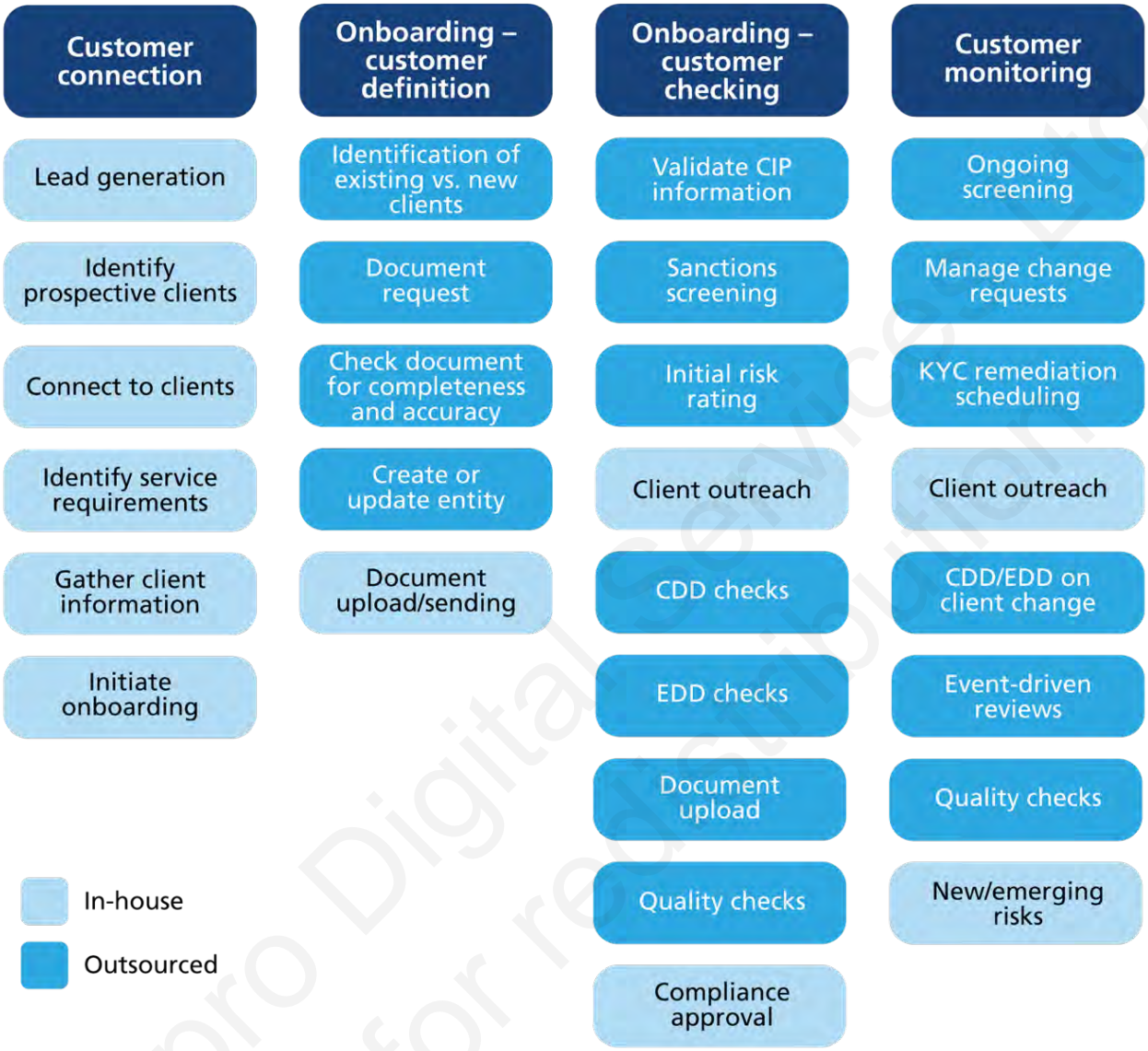
Cloud-based services also offer a high degree of security and reliability.

Customer data is typically stored in encrypted form, and access is controlled through user authentication and authorization. In addition, cloud-based services can be accessed from anywhere, which is convenient for both financial institutions and their customers. Finally, cloud-based services are constantly evolving, and providers can regularly offer new features and capabilities on a regular basis.

The growth in cloud-based solutions has been accompanied by an uptick in outsourcing. Financial institutions are seeking to reduce in-house involvement in non-core AML compliance activities by outsourcing them to external providers. For many firms, outsourcing is a cost-effective method of managing AML compliance and mitigating their risk of fines. The elements of AML/KYC activities that lend themselves to outsourcing tend to be low-risk, with fewer decision-making or human-centric elements involved. For example, service companies are well placed to manage such labor-intensive and routine tasks as customer due diligence, enhanced due diligence and verifying customer identification. Only when risk scores are particularly high are these processes typically redirected to in-house staff.

Notably, when outsourcing, financial institutions do not cede ultimate responsibility and control to the organization doing the work. Firms must therefore be careful about which tasks they outsource, to ensure they stay in compliance with regulations. Final sign-off or initiating contact with clients (to update documents, for example) must be done in-house. Any activities that include the filing of sensitive reports, such as internal investigations of suspicious activities, are not conducive to outsourcing. These types of inquiry could involve employee interviews, document evaluations and the preparation of reports, all of which call for confidentiality. Figure 2 provides a more detailed overview of the activities typically outsourced or performed in-house.

Figure 2: Outsourced vs. in-house activities during the KYC process



Source: Chartis Research

Other themes in the KYC solutions market

Geographical variation

Geographical variation is common in the KYC process. Because institutions must account for both global and regional regulation, their risk profiles and compliance requirements change from country to country. The level of geographic variation has increased, and expectations are that it will continue to do so. While US sanctions remain the primary driver for the market for compliance solutions, there

is currently no comprehensive international framework for regulating sanctions, creating a great deal of variation across countries. This variation is likely to increase in the future as more countries adopt their own sanction regimes.

The rise of such regional organizations as the African Union and the Association of Southeast Asian Nations is likely to lead to more regional cooperation on how to address sanctions. In addition, the increasing use of sanctions by US and European Union regulators, among others, could result in the development of more sophisticated national regimes. Moreover, the increasing use of sanctions by international organizations such as the United Nations may lead to the development of more comprehensive international sanctions frameworks.

The implications of variation

The increased geographical variation in sanctions regulation could have a number of implications:

- It could make it harder to enforce sanctions.
- It may lead to a greater risk of abuse, because some countries may be tempted to use sanctions for political reasons, rather than to address legitimate security or humanitarian concerns.
- It is likely to make cooperation between regulators more difficult to achieve: some countries will be less inclined to agree to cooperate on a particular issue if they know they will be at a disadvantage.

Chartis anticipates that these dynamics will lead to greater geographical segregation of vendor capabilities, alongside the growing variation in regional data environments, as discussed in Chartis' ***KYC/AML Data Solutions, 2022: Market Update and Vendor Landscape*** report.

Beyond KYC: more detail on counterparties

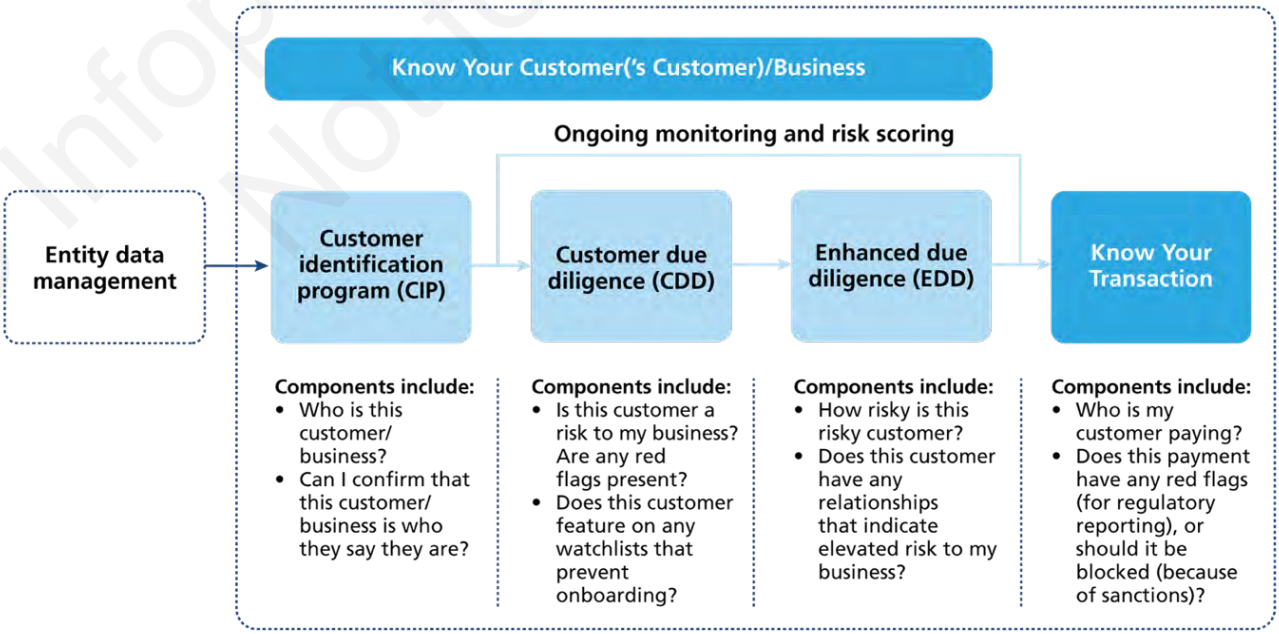
As the level of data required for KYC processes has increased, institutions have considered more sophisticated ways of quantifying their counterparties. These have led to the proliferation of several different varieties of KYC, as financial institutions have built out more detailed and complex KYC systems within their technology architecture and compliance frameworks. Among the most prominent of these varieties are (see Figure 3):

Know Your Business (KYB). KYB is the basis for identifying high-risk and restricted entities at the point of customer onboarding and throughout the customer lifecycle. Using company risk information, compliance teams can:

- Conclusively verify a corporate entity's identity.
- Resolve the entity to a full corporate hierarchy, parent corporation and set of shareholders.
- Identify beneficial owners.
- Pinpoint relationships between business entities.
- Perform in-depth research, to reveal relevant information for financial crime investigations and to validate onboarding decisions (using enhanced due diligence).

Know Your Customer's Customer (KYCC). The process of identifying entities that are farther down the chain from their immediate counterparties. This involves determining whether an institution is interacting with entities that are one or more steps removed from it, and which could be dangerous from a risk and/or sanctions perspective. This is a complex procedure that becomes more challenging the more steps an institution chooses to look down its relationship chain.

Figure 3: Varieties of KYC – KYB and KYCC



Source: Chartis Research

Jump to top

Vendor landscape

General technology trends

The KYC space continues to expand, as does the variety of entrants and technological strategies within it. Some notable technology themes include the following:

- **The cloud has become a constant presence**. Almost all vendors now have a cloud strategy. Low entry costs, scalability and speed to market are seen as the key competitive advantages for vendors offering cloud solutions. In addition, the use of APIs within the cloud and containerizations means that firms can more easily access third-party data providers, other vendors or service capabilities, and from a wider range of physical locations.
- **Workflow strategies have diversified**, and the variety of workflow capabilities has grown. Low-code and no-code approaches, in particular, have enabled firms to employ graphical user interfaces (GUIs) so they can use pre-built code for document management, data capture and IDV. Several firms in the space market, alongside agile and legacy workflow players, now use a no-code approach as their primary differentiator and selling point.
- **IDV vendors are moving into KYC**. Vendors offering bespoke IDV solutions are building out compliance capabilities and moving into the KYC marketplace. The transition to digital methods of customer IDV and validation during the onboarding process has accelerated. Biometrics and facial recognition have been key tools in onboarding customers quickly and remotely, and Chartis has seen several dedicated IDV firms enter the KYC and onboarding space.
- **APIs and connectors are becoming more standardized**, ensuring that deployments are as modular as possible. APIs, which are increasingly flexible, organized and well-documented, can be integrated more easily with other vendors' core infrastructure to help them meet new requirements. In addition, hybrid services and technology are becoming more common, and partnerships between firms (as well as acquisitions in the market) have continued apace.

Jump to top

Chartis RiskTech Quadrant® and vendor capabilities for KYC solutions, 2022

Figure 4 illustrates Chartis' view of the vendor landscape for KYC solutions. Table 1 lists the assessment criteria we used for this analysis, and Table 2 lists the corresponding vendor capabilities.

Figure 4: RiskTech Quadrant® for KYC solutions, 2022

Source: Chartis Research

Table 1: Assessment criteria for vendors of KYC solutions, 2022

Completeness of offering	Market potential
Reporting and dashboarding	Customer satisfaction
KYC risk scoring	Market presence
Customer profile enrichment with additional data	Growth strategy
Customer onboarding	Business model
	Financials

Source: Chartis Research

Table 2: Vendor capabilities for KYC solutions, 2022

Vendor	Reporting and dashboarding	KYC risk scoring	Customer profile enrichment with additional data	Customer onboarding
Alloy	**	**	**	**
AML Partners	****	***	***	***
Appian	****	**	**	****
BasisTech	**	*	**	***
ComplyAdvantage	**	****	***	***
Diligent	**	**	*	****
Eastnets	**	**	***	**
Encompass	**	***	****	***
Fenergo	****	****	****	****
FIS	**	**	***	****
Fiserv	**	***	**	***
iMeta	**	***	****	***
KYC Portal	***	**	****	****
LexisNexis Risk Solutions	**	**	****	**
Manipal Group	***	***	***	**
NetReveal	**	****	**	***
NICE Actimize	**	****	***	***
Oracle	**	****	***	***
Pega	****	****	***	****
PwC	****	***	***	****
Quantexa	**	****	****	***

RiskScreen	**	***	***	****
S&P Global	****	**	***	****
SAS	***	****	***	***
Shufti Pro	**	*	**	****
Sigma Ratings	***	***	****	**
Silent Eight	**	**	****	****
smartKYC	****	***	****	***
SymphonyAI Sensa	****	****	***	*
Veriff	*	***	**	****
Vneuron	***	***	***	***
Zoloz	**	**	***	***

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

Source: Chartis Research

Quadrant commentary

The KYC quadrant is once again characterized by a proliferation of vendors: the category leader space has become particularly diverse, as a number of firms have established solutions that cover many discrete parts of the KYC completeness of offering, either through organic development or acquisition. Data firms have built out their technology solutions, while vendors of enterprise solutions have developed their analytics, and service firms have extended their solution offerings.

Agile workflow and automation have also been key areas of focus, and several players in the market are making a significant impact in terms of their completeness of offering scores. In general, diversity of solution offering is a noteworthy factor: many solutions in the best-of-breed and point-solution categories have specific areas of focus, such as the investigations process, workflow assistance in the onboarding process, IDV or enhanced due diligence. The continued growth in diversity within the quadrant, the competition now occurring in a growing number of sub-segments, and ongoing regulatory attention indicate that the KYC solutions market will remain vibrant for several years.

The managed services dynamic continues to influence the landscape as leading managed service providers (MSPs) assemble a multitude of software-as-a-

service/on-premises solutions into an end-to-end system architecture. Their purchasing decisions also inform the market: they are constantly evaluating their technology choices and bottom line; if new technology offers significant improvements, they will consider integrating it into their stacks. MSPs will consider new tech if it can significantly reduce costs or just augment their existing capabilities. As they aim to provide best-in-class solutions to clients, their choice of vendors to partner with or use in service offerings will have a significant effect on the market presence of vendors across the KYC marketplace.

Jump to top

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' 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 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®

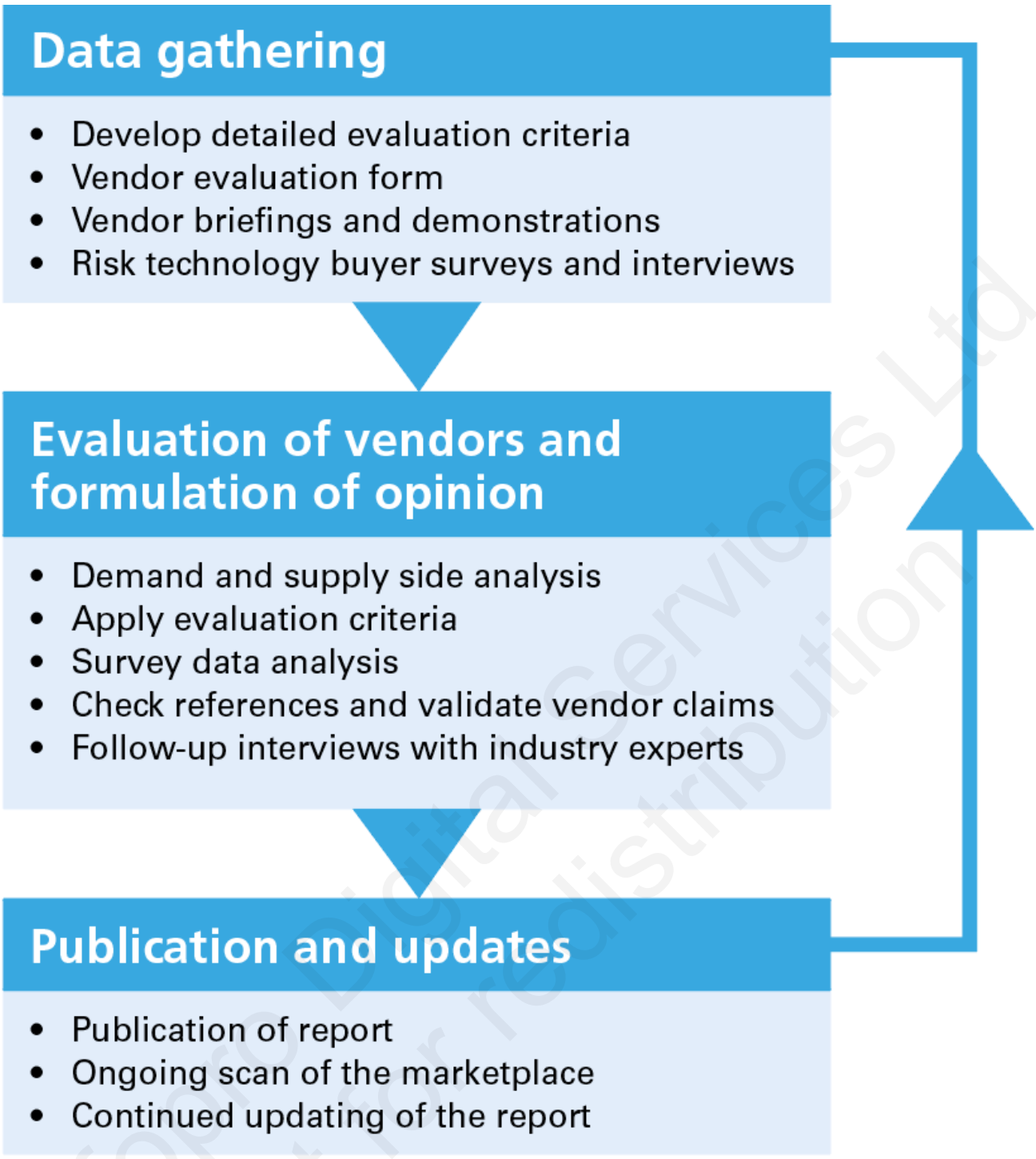
Chartis seeks to include risk technology vendors that have a significant presence in a given target market. The significance may be due to market penetration (e.g., large client base) or innovative solutions. Chartis does not give preference to its

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 5 below describes the research process.

Figure 5: 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.

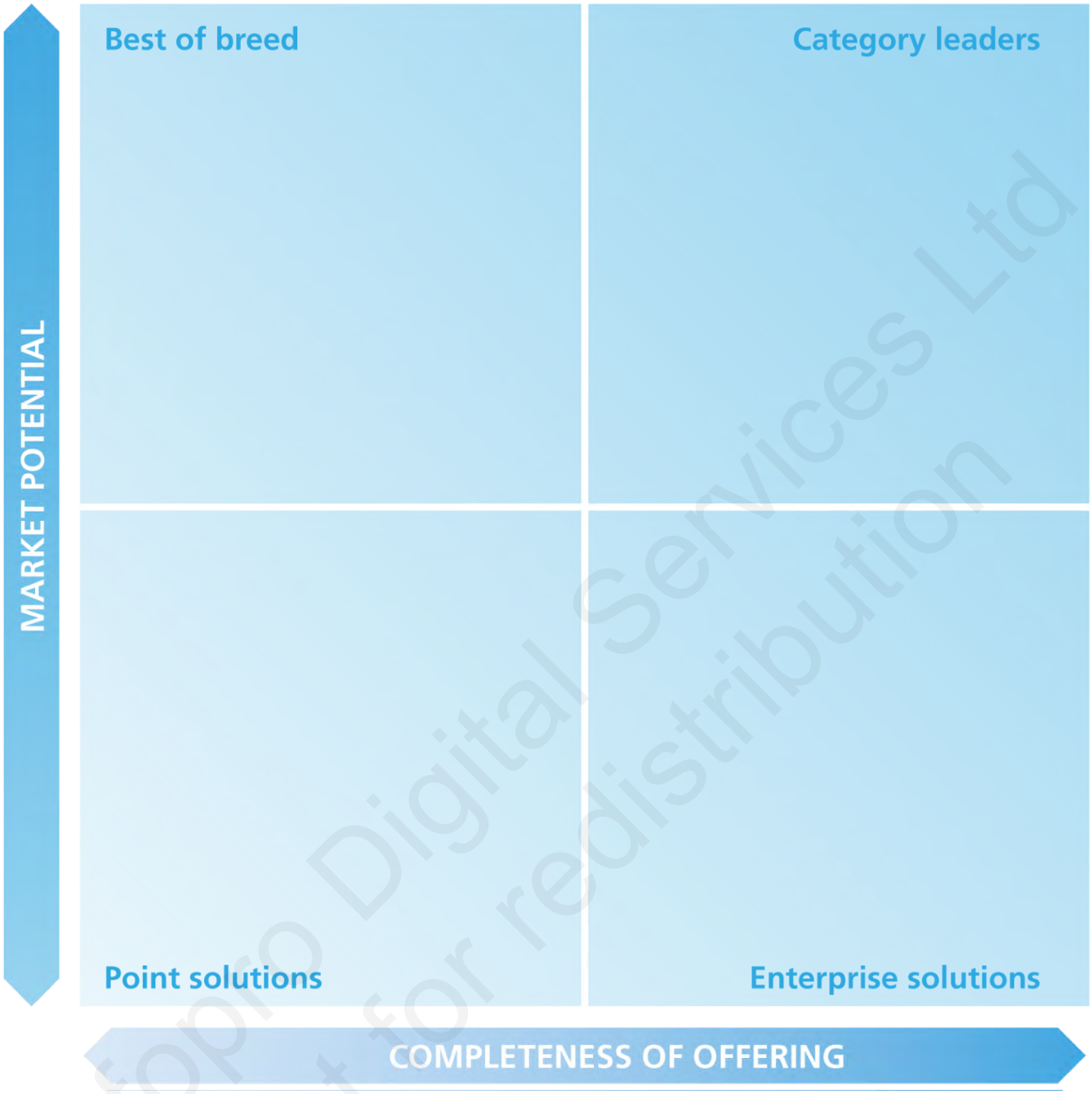
- **Interviews with subject matter experts.** Once a research domain has been selected, Chartis undertakes comprehensive interviews and briefing sessions with leading industry experts, academics and consultants on the specific domain to provide deep insight into market trends, vendor solutions and evaluation 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 6) evaluates vendors on two key dimensions:

1. Completeness of offering
2. Market potential

Figure 6: 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 number 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 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 varies for each subject area, but special attention is 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.

Jump to top

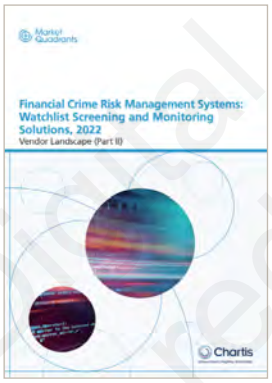
Further reading

KYC/AML Data Solutions, 2022: Market Update and Vendor Landscape

KYC/AML Software Solutions, 2020: Market Update and Vendor Landscape

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

Financial Crime Risk Management Systems: Watchlist Monitoring Solutions, 2022; Market Update and Vendor Landscape



Financial Crime Risk Management Systems: Watchlist Screening and Monitoring Solutions, 2022; Vendor Landscape (Part II)

Big Bets 2022

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