Market Quadrants

KYC Data and Solutions, 2023

Market Update and Vendor Landscape

Chartis

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:

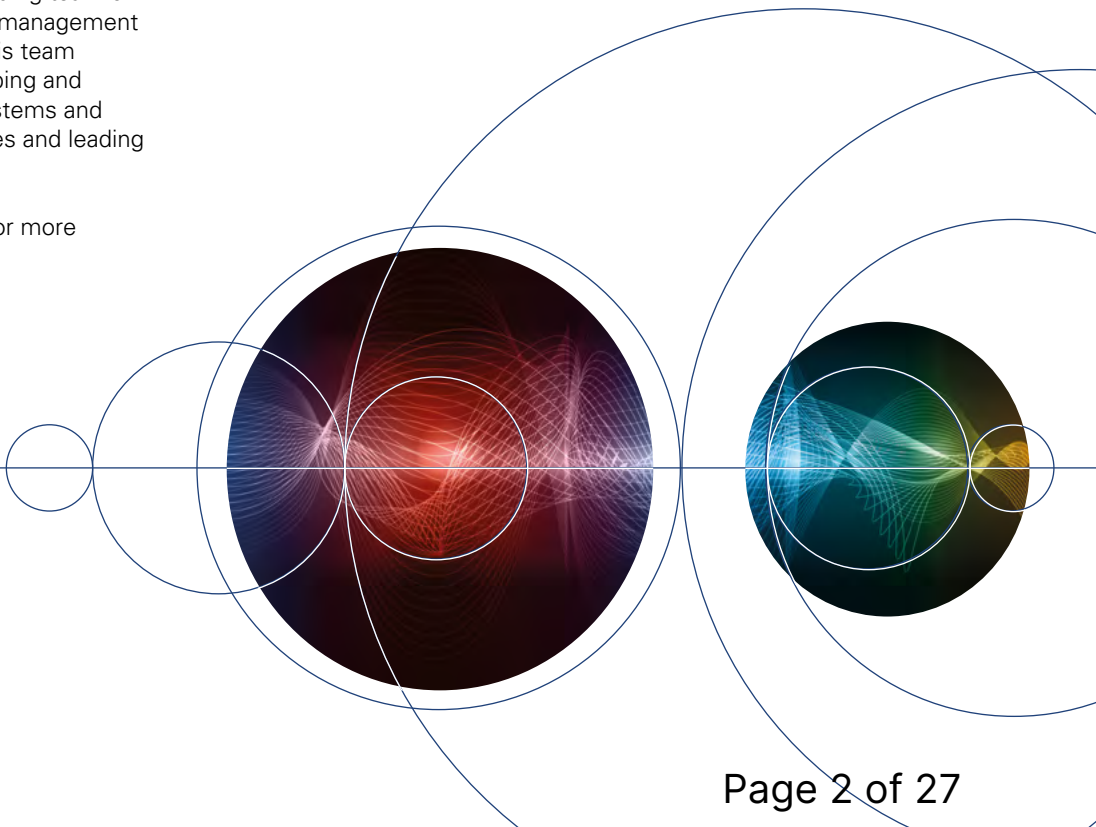
- Credit risk.
- Operational risk and governance, risk management and compliance (GRC).
- Market risk.
- Asset and liability management (ALM) and liquidity risk.
- Energy and commodity trading risk.
- Financial crime, including trader surveillance, anti-fraud and anti-money laundering.
- Cyber risk management.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



29 SEP 2023

Market Quadrants Report

Authors
Phil Mackenzie and Ahmad Kataf

Jump to: Market update | Vendor landscape | Chartis RiskTech Quadrant® and tables – KYC data solutions | Chartis RiskTech Quadrant® and tables – KYC solutions | Methodology

Executive summary

This report updates our previous research into the KYC solutions landscape,[1] and provides a concise overview of our main findings and insights.

Several important developments are driving change in the areas of Know Your Customer (KYC) and anti-money laundering (AML) compliance. The US remains a dominant force in shaping sanctions and regulatory measures, helping to push sanctions deeper into the global supply chain. Complex products and services have further complicated the processes of identifying and managing risks, including those related to money laundering and terrorist financing. To mitigate these risks, companies are prioritizing supply chain due diligence, which increasingly encompasses supplier and customer assessments, transaction monitoring and compliance programs. This is causing financialized corporations to intensify their focus on compliance and customer onboarding to address the risks inherent in the supply chain risks and complex transactions.

The data landscape has also become more complex. Following a ruling by the European Court of Justice (ECJ), efforts in the European Union (EU) to enhance transparency through beneficial ownership records have encountered setbacks. While public access to these records has been restricted, certain entities, including financial institutions and investigative organizations, have retained access. As the corporate data landscape becomes more complex, firms will have to adjust their relevant solutions in response.

The cloud dynamic has also complicated matters. New regulations in the EU (and a general understanding that the cloud is not always a cost-saving 'magic bullet') have led to a slowing in the monotonic growth of cloud solutions. More firms are now looking at hybrid solutions or staying with on-premise deployments.

Among solution vendors, some firms are cautiously exploring the use of generative artificial intelligence (AI) in KYC processes, particularly for generating reports and analyzing negative news. While this technology offers new possibilities, it requires careful implementation and meticulous error-checking.

The RiskTech Quadrant® for KYC data solutions continues to evolve, driven by network effects – larger data vendors are acquiring smaller ones, enriching their offerings. The depth of data and its geographical specificity are expanding to encompass such areas as bribery, corruption, forced labor and regional specifics.

KYC solutions, meanwhile, are becoming more complete, and now emphasize case management, workflow, analytics, screening and due diligence. For category leaders, market presence and growth are now essential.

As the financial landscape continues to evolve, KYC and AML compliance remain critical for financial institutions and vendors alike. To stay competitive, and compliant, it is vital that all firms understand – and adapt to – these trends.

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 best for buyers, depending on their implementation strategies.

This report covers the following providers of KYC and KYC data solutions:[2] Alloy, AML Partners, Appian, ComplyAdvantage, Deep Pool, Dow Jones Risk & Compliance, Eastnets, Encompass, Feedzai, Fenergo, FIS, GBG, Giant Oak, IMTF, Innovative Systems, Kharon, KYC2020, KYC Portal, LexisNexis Risk Solutions, Manipal Group, Moody's, Muinmos, NICE Actimize, Oracle, Pega, Quantifind, Ripjar, RiskScreen, Rozes, SAS, Sigma Ratings, smartKYC,

SymphonyAI, Vneuron and Xapien.

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 market dynamics

The US is helping to drive sanctions deeper into the supply chain

Several key developments in the US have helped to increase the level of sanctions and financial regulation in the country and elsewhere:

- The Financial Crimes Enforcement Network (FinCEN) published its final ruling on beneficial ownership information (BOI) provisions in September 2022.
- The US Treasury's National Strategy for Combatting Terrorist and Other Illicit Financing was announced in May 2022. This strategy aims to increase transparency and strengthen US AML/combatting the financing of terrorism (CFT) regulations by closing loopholes in the country's financial system.
- In February 2023, the White House announced a range of new economic restrictions. These included new export restrictions targeting Russia's defense and energy sectors, and a crackdown on attempts by third parties to evade US sanctions on Russia. The announcement also included a joint initiative with the UK to impose sanctions on Russian cybercriminals.

These new restrictions have helped to drive sanctions – as a tool – deeper into the supply chain. **The restrictions** target companies involved in the production of weapons and materials sent to Ukraine, as well as those supporting the Russian economy. They are also increasingly aligned with strategic priorities – in this case, depriving Russia of the equipment, technology and services it needs for its military operations. Additional, lesser expansions of restrictions have sought to address other issues, including the US focus on **forced labor in Xinjiang** and the **fentanyl supply chain.**

The problem for financial institutions and vendors is that modern supply chains are complex. The increasing globalization of trade has led to more interconnected supply chains, which now include a growing number of stakeholders across suppliers, manufacturers, distributors and retailers. In addition, the increasing complexity of products and services has made tracing these networks more of a challenge.

This complexity can make it difficult for firms to identify and manage risks associated with money laundering and terrorist financing. Moreover, companies' supply chains may involve transactions with parties in countries that are subject to sanctions, increasing the risk of non-compliance.

To mitigate these risks, firms are increasingly focusing on supply chain due diligence. This includes conducting due diligence on suppliers and customers, monitoring transactions for suspicious activity and implementing compliance programs.

EU confusion on beneficial ownership makes the data landscape more challenging

As sanctions have become a more politically potent tool, there has been a heightened focus among firms on providing more detailed, complete corporate information. This move has typically been spearheaded by institutions in Europe and the UK. The UK's Economic Crime (Transparency and Enforcement) Act of 2022, for example, has increased the application of financial and trade sanctions following Russia's invasion of Ukraine. The act is designed to prevent foreign owners from laundering their money through UK property, by establishing a new register of overseas entities that records beneficial ownership.

This movement has slowed, however. According to **a ruling by the ECJ**, public access to beneficial ownership registries in the EU has been revoked because of concerns about privacy and data protection under the EU Charter of Fundamental Rights. The ECJ's ruling states that opening these registries to the general public interferes with individuals' rights to privacy and personal data protection. However, the court confirmed that some entities have a legitimate interest in accessing beneficial ownership information:

- Journalists.
- Civil society organizations investigating or campaigning on crime and corruption.
- Financial institutions and other entities with AML obligations.

Ideally, this would have little effect on vendors and financial institutions, as both can prove that they have a legitimate interest. But this space is typically governed by caution: small regulatory changes can cause strong effects as participants try to avoid any potential negative consequences. Notably, the ruling has prompted some European countries, including Luxembourg, Austria, Germany, the Netherlands and Ireland, to take their registries offline. The upshot of this for vendors and financial institutions is that the source data, and the processes for determining corporate ownership and structures, will become more complex, as more information 'black holes' potentially emerge in the corporate landscape. To address this, firms will have to rely more on alternative data sources, and develop new ways to infer information from pre-existing sources.

More penalties in EMEA

According to **a report by *Global Investigations Review***, despite a global decrease in AML enforcement actions and penalties in 2021, they more than tripled in Europe, the Middle East and Africa (EMEA) compared with the year before. (Notably, demand for AML solutions has increased in the Middle East in particular.) This is largely because a few countries in the region have maintained their momentum in terms of regulatory activity, alongside the ongoing extraterritorial reach of the US.

Financialized corporations are the focus – and the customers – for complex KYC solutions

Large corporates have generally had to pay more attention to their compliance and customer onboarding, and are increasingly becoming part of the buyer landscape for KYC solutions. The need to address supply chain risk has brought them more into the sanctions and compliance space – they are involved in complex transactions with multiple parties, making it difficult to identify and manage risks.

For their part, small and medium-sized enterprises may have a more complex ownership structure and a higher concentration of buyers and

suppliers. And small enterprises may have fewer personnel and financial resources to carry out due diligence. At the same time, they often have greater flexibility in terms of policymaking and implementation, and may have fewer impacts or suppliers to manage compared with larger enterprises.

Geographical alignment of sanctions – increasingly complex to manage

The most complex driver of sanctions strategies at present is the alignment between different countries – emphasized by the shift in beneficial ownership strategies. The current sanctions environment is broadly aligned across countries and regions. Multiple countries, for example, including the US, members of the EU, Japan and South Korea, have imposed sanctions on North Korea in response to its nuclear weapons and ballistic missile programs. While the specific measures taken may vary, the overall goal of denuclearization has led to some alignment of the sanctions being imposed.

Similarly, the Iran nuclear deal, formally known as the Joint Comprehensive Plan of Action (JCPOA), involved the US, members of the EU and other major world powers. While the agreement was in place, sanctions against Iran were coordinated and aligned among these parties, with the common goal of limiting the country's nuclear capabilities.

However, there are also areas where sanctions are misaligned. Historically, the US has maintained a long-standing embargo on Cuba, while the EU and other countries have not imposed similar comprehensive sanctions. This has led to differences in policy and sanctions regimes between the US and many other nations. Sanctions on Venezuela have also differed between the US and the EU. While both regions have imposed sanctions on individuals and entities associated with the Venezuelan government, the scope and objectives of these sanctions have not always been fully aligned. The US has taken a more aggressive stance that includes oil-related restrictions, while the EU has pursued diplomatic efforts alongside sanctions.

Financial institutions and vendors should be aware of any potential splits between the major sanctioning bodies. At the moment, the US leads and the world follows, but any kind of multi-polar sanctioning regime makes sanctions management even more complex.

Jump to top

Vendor landscape

Technology dynamics

Regulatory and cost drivers are complicating the cloud option

Companies' appetite for cloud solutions – with benefits that include scalability, flexibility and cost-effectiveness – has grown in recent years. But firms and regulators are increasingly concerned about data privacy and security issues.

- The EU recently proposed the draft European Data Act, which **aims to facilitate** access to and use of data generated by Internet of Things devices and related services by companies, public authorities and individuals. The EU plans to compile a set of rules in the form of an EU 'cloud rule book' with guidance on the public procurement of data-processing services. The **rule book will provide** a single European framework with binding and non-binding rules for cloud service users and providers in Europe.
- The EU's Cybersecurity Act establishes the legal basis for the EU-wide certification of cloud providers. This **will be elaborated on** by the EU's cybersecurity agency, ENISA, via secondary laws.

Consequently, as the regulatory landscape has become more complex, more financial institutions (and, by extension, the vendors serving them) have become wary of deploying cloud-based KYC solutions. This runs alongside other, similar cloud-related trends. In previous years, we have seen an almost monotonic increase in demand for cloud platforms. But this has started to slow, as firms accustomed to working within the financial institutions' technology perimeter have often found that cost savings have not been as high as promised. One of the primary benefits of the cloud, for example, has been its capacity to scale in response to internal and external changes, and firms with more static workloads have been unable to take advantage of this.

Nevertheless, some companies have prioritized the quick installation times and potential flexibility of cloud offerings: challenger banks and financial institutions that are expanding or conducting onboarding drives are the main beneficiaries of this approach. But while the cloud remains a valuable tool and deployment option for many vendors, some have been retrenching

with an on-premise strategy.

Elsewhere, however, the application programming interface (API) and connectivity dynamics of the cloud continue to foster cross-pollination between firms. KYC vendors have been actively integrating more APIs and enhancing their connectivity with third-party data services (including those from credit bureaus, government databases, identity verification providers and other KYC vendors) to improve their operations. This integration allows KYC vendors to access real-time data for the purposes of identity verification, risk assessment and compliance.

Generative AI: cautious first steps

Some solution vendors have announced their first forays into the use of generative AI within the KYC space. Most are understandably cautious. The predictive nature of most large language models (LLMs) means that they are often likely to come up with 'common' answers to questions (i.e., a probabilistic determination of the most frequent answer) and lack the ability to error-check their own work.

Nevertheless, Chartis has seen some firms move into the space with report-generation capabilities for suspicious activity reports (SARs) (using LLMs to auto-generate reports based on existing data), and in the negative news space (using LLMs to populate negative news reports).

With commercially available LLMs such as GPT-4 dominating much of the discourse, firms are pursuing different options for using these capabilities:

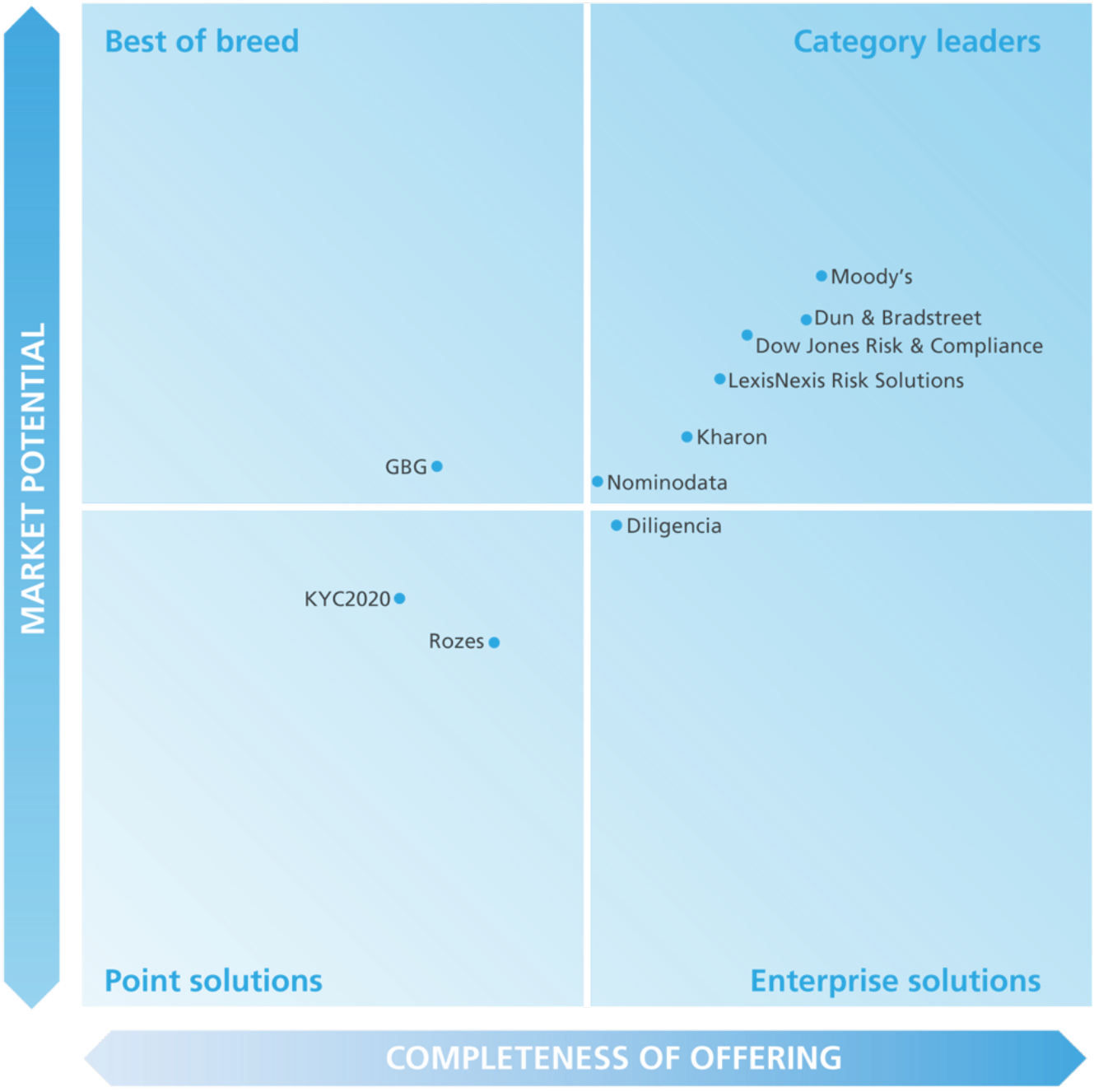
- Using an API to provide services from an established LLM (such as GPT-4), which can then be attached to a negative-news or report-generation platform.
- Using APIs to provide a choice of LLMs (BLOOM, PaLM or GPT-4, for example), enabling users to select those that they feel are more suited to their purposes.
- Developing their own LLM. While the time and development costs for building an LLM at scale are prohibitive, some vendors have developed (or are in the process of developing) their own LLMs. One benefit of this approach is that these LLMs can be better suited to their target market (adverse media, for example), although they have less flexibility (in terms of queries) than commercial LLMs.

Jump to top

Chartis RiskTech Quadrant® and vendor capabilities for KYC data solutions, 2023

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

Figure 1: RiskTech Quadrant® for KYC data solutions, 2023



Source: Chartis Research

Table 1: Assessment criteria for vendors of KYC data solutions, 2023

Completeness of offering	Market potential
Sanctions and watchlist data	Customer satisfaction
Negative news and PEPs	Market penetration
Traditional ID	Growth strategy
Electronic and digital ID	Business model
Corporate structure	Financials
Entity relationships	
Trade-related financial crime risk	
High-risk business	

Source: Chartis Research

Table 2: Vendor capabilities for KYC data solutions, 2023

Vendor	Sanctions and watchlist data	Negative news and PEPs	Traditional ID	Electronic and digital ID	Corporate structure	Entity relationships	Trade-related financial crime risk	High-risk business
Diligencia	***	**	*	*	****	****	**	**
Dow Jones Risk & Compliance	****	****	*	*	****	****	****	****
Dun & Bradstreet	****	****	**	**	****	****	****	****
GBG	**	**	****	****	**	**	*	**
Kharon	****	**	*	*	****	****	****	***
KYC2020	****	****	*	*	*	*	**	***
LexisNexis Risk Solutions	****	****	****	****	***	***	**	***
Moody's	****	****	****	**	****	****	****	****
Nominodata	****	****	**	**	**	**	****	****
Rozes	**	**	*	**	****	**	*	**

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

Source: Chartis Research

Quadrant dynamics for KYC data solutions

The 'network effect' dynamics of the KYC data solutions quadrant remain intact. Significant network effects are at play, enabling larger data vendors to acquire smaller ones to further enrich their own offerings. This also leads to a relatively strong correlation between market potential and completeness of offering.

The depth of the data being offered continues to expand. Major and minor vendors alike are looking to establish footholds in new areas. These are not always specifically compliance- and/or AML-focused, but bring in information from adjacent areas. This allows financial institutions to create more complete pictures of their more complex counterparties or onboarded individuals. **These datasets include bribery and corruption**, forced labor and supply chain datasets.

The geographical specificity of the data on offer has also increased. As ultimate beneficial ownership data has become more difficult to obtain, more firms have been building out data that focuses on specific local factors, whether these relate to regional crime groups, local registry data that cannot be obtained online or integrations with regional identity datasets.

The landscape continues to be dominated by a few major vendors. With ongoing voracious growth in demand from financial institutions in terms of the size and complexity of the data, however, new entrants and established players will continue to carve out niches and expand this quadrant.

Jump to top

Chartis RiskTech Quadrant® and vendor capabilities for KYC solutions, 2023

Figure 2 illustrates Chartis' view of the vendor landscape for KYC data. Table 3 lists the completeness of offering and market potential criteria we used to assess the vendors. Table 4 lists the vendor capabilities in this area.

Figure 2: RiskTech Quadrant® for KYC solutions, 2023

Source: Chartis Research

Table 3: Assessment criteria for vendors of KYC solutions, 2023

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

Source: Chartis Research

Table 4: Vendor capabilities for KYC solutions, 2023

Vendor	Reporting and dashboarding	KYC risk scoring	Customer profile enrichment with additional data	Customer onboarding	Customer maintenance
Alloy	**	***	***	**	**
AML Partners	****	***	***	***	***
Appian	****	***	***	****	****
ComplyAdvantage	**	****	***	***	**
Deep Pool	***	****	***	***	***
Dow Jones Risk & Compliance	***	**	****	***	**
Eastnets	***	***	***	***	***
Encompass	***	**	****	****	***
Feedzai	***	****	***	**	**
Fenergo	****	****	***	****	****
FIS	***	***	***	****	***
GBG	***	***	****	***	****
Giant Oak	***	****	**	**	***
IMTF	***	***	****	***	**
Innovative Systems FinScan	***	***	****	***	**
Kharon	***	**	****	***	***
KYC2020	***	***	****	***	**
KYC Portal	****	***	****	****	***
LexisNexis Risk Solutions	**	***	****	**	**
Manipal Group	***	***	**	****	**
Moody's	***	**	****	***	****
Muinmos	****	**	****	****	**
NICE Actimize	***	****	***	***	***
Oracle	***	****	***	****	****
Pega	***	***	***	****	***
Quantifind	***	****	****	*	**
Ripjar	***	***	****	***	**
RiskScreen	**	***	***	****	**
Rozes	**	*	***	**	**
SAS	***	****	***	***	***
Sigma360	***	****	****	**	**
smartKYC	****	***	****	***	****
SymphonyAI	***	****	***	***	**
Vneuron	***	***	***	***	****
Xapien	****	***	***	***	***

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

Source: Chartis Research

Quadrant dynamics for KYC solutions

Bigger and more. In the KYC solutions quadrant, we can again see a proliferation of vendors. Several firms have established solutions that cover various aspects of KYC completeness, achieving this with organic development and acquisitions. Data firms have expanded their technological solutions, enterprise solution providers have enhanced their analytics capabilities, and service-oriented firms have broadened their solution offerings.

Scale and completeness increase across the board. Notably, while KYC vendors have often been characterized by a component approach, many firms have continued to build out their KYC solutions into more complete offerings. Increasingly, having a presence across case management and workflow, analytics, screening and due diligence can be seen as 'table stakes' for entry into the space. Similarly, ongoing expansion in the space has meant that significant growth and market presence are now essential for firms in the category leaders quadrant; numerous vendors can point to double-digit year-on-year growth.

Vertical specificity. While some firms have had notable success jumping between verticals to offer specific services, this has typically occurred within a relatively tight selection of capabilities (such as data analytics). The scale and completeness of solutions have increased, but this mostly occurs as firms become more familiar with providing for a given subset of customers, whether these are in the wholesale, corporate and investment, or retail sectors.

Data analytics continue to evolve. While network and graph analytics are more standardized approaches for firms building connections between counterparties, strategies around linguistic data are proliferating. These strategies include more sophisticated search and matching, and better abilities to extract contextual information from sources such as negative news media. Chartis expects this to be an area where generative AI could have a strong impact going forward.

As employee costs remain high, technology revenues are a key signifier of success. As managed services and technology continue to combine in the KYC space, many firms are looking to build modular, services-oriented offerings, using humans on the ground to modify and manage their technology. While this can bring growth, companies that have achieved higher profit margins have been able to do so via technology revenues, and in this iteration of the report, these firms were some of the best performers.

Jump to top

Notes

1. See the Chartis reports ***KYC Solutions, 2022: Market Update and Vendor Landscape*** and ***KYC/AML Data Solutions, 2022: Market Update and Vendor Landscape***.

2. Note that references to companies in the text of this report do not constitute endorsements of their products or services by Chartis.

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.

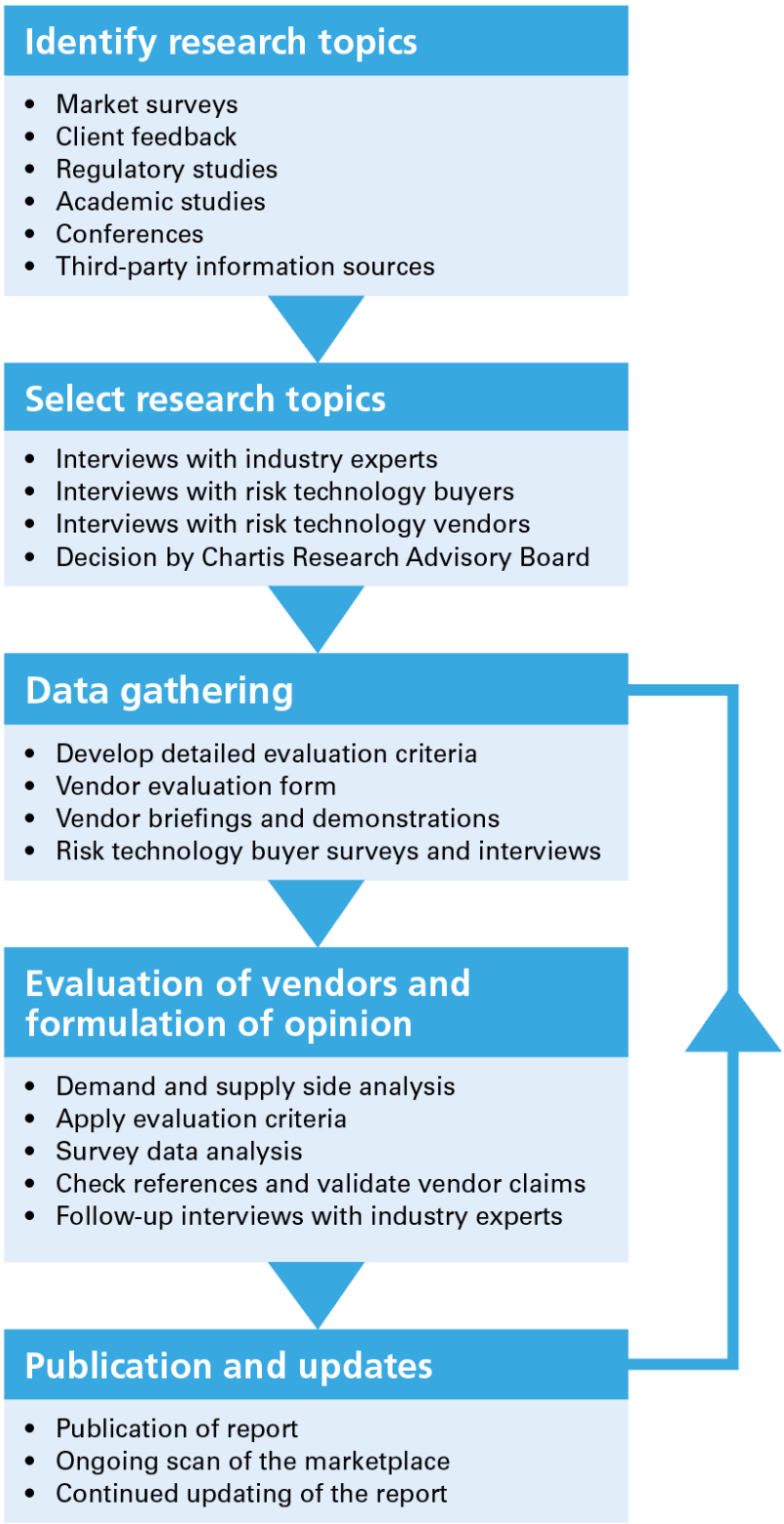
Inclusion in the RiskTech Quadrant®

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 3 below describes the research process.

Figure 3: 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):

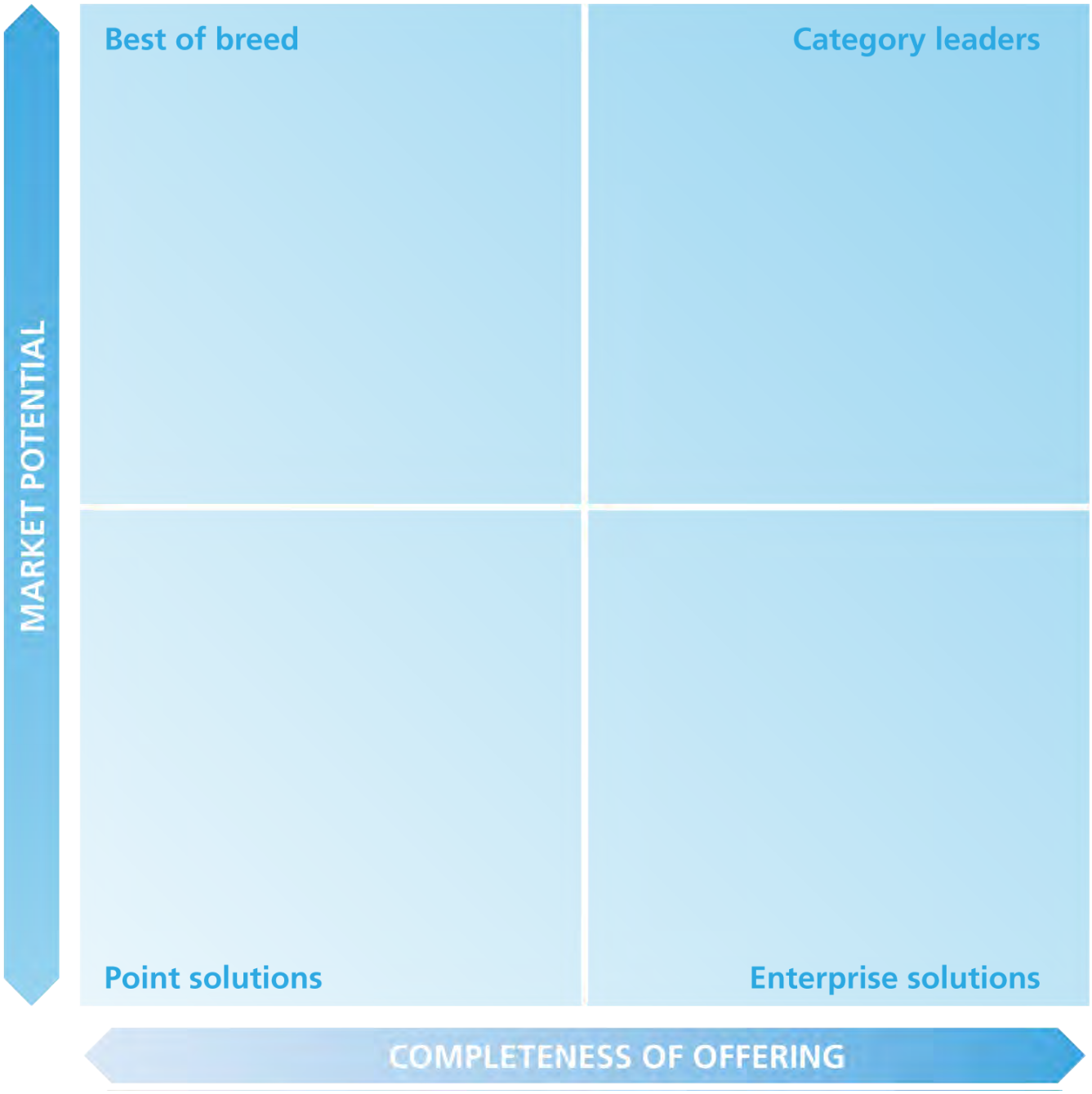
- **Chartis vendor evaluation forms.** A detailed set of questions covering functional and non-functional aspects of vendor solutions, as well as organizational and market factors. Chartis' vendor evaluation forms are based on practitioner-level expertise and input from real-life risk technology projects, 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 4) evaluates vendors on two key dimensions:

1. Completeness of offering
2. Market potential

Figure 4: 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.

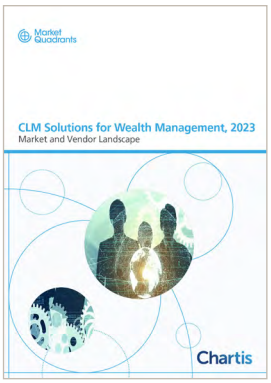
Category leaders will typically benefit from strong brand awareness, global reach and strong alliance strategies with leading consulting firms and systems integrators.

Jump to top

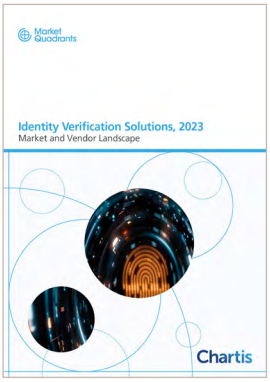
Further reading

KYC Solutions, 2022: Market Update and Vendor Landscape

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

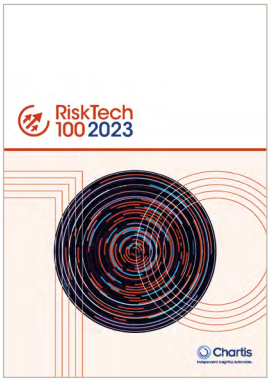


CLM Solutions for Wealth Management, 2023: Market and Vendor Landscape



Identity Verification Solutions, 2023: Market and Vendor Landscape

Payment Risk Solutions, 2023: Market and Vendor Landscape



RiskTech100 2023

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