Market Quadrants

Financial Crime Risk Management Systems: AML and Watchlist Monitoring

Market Update and Vendor Landscape, 2019

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 'Terms and conditions' on **www.chartis-research.com**.

RiskTech100®, RiskTech Quadrant®, FinTech Quadrant™ and The Risk Enabled Enterprise® are Registered Trade Marks of Infopro Digital Services Limited.

Unauthorized use of Chartis' name and trademarks is strictly prohibited and subject to legal penalties.

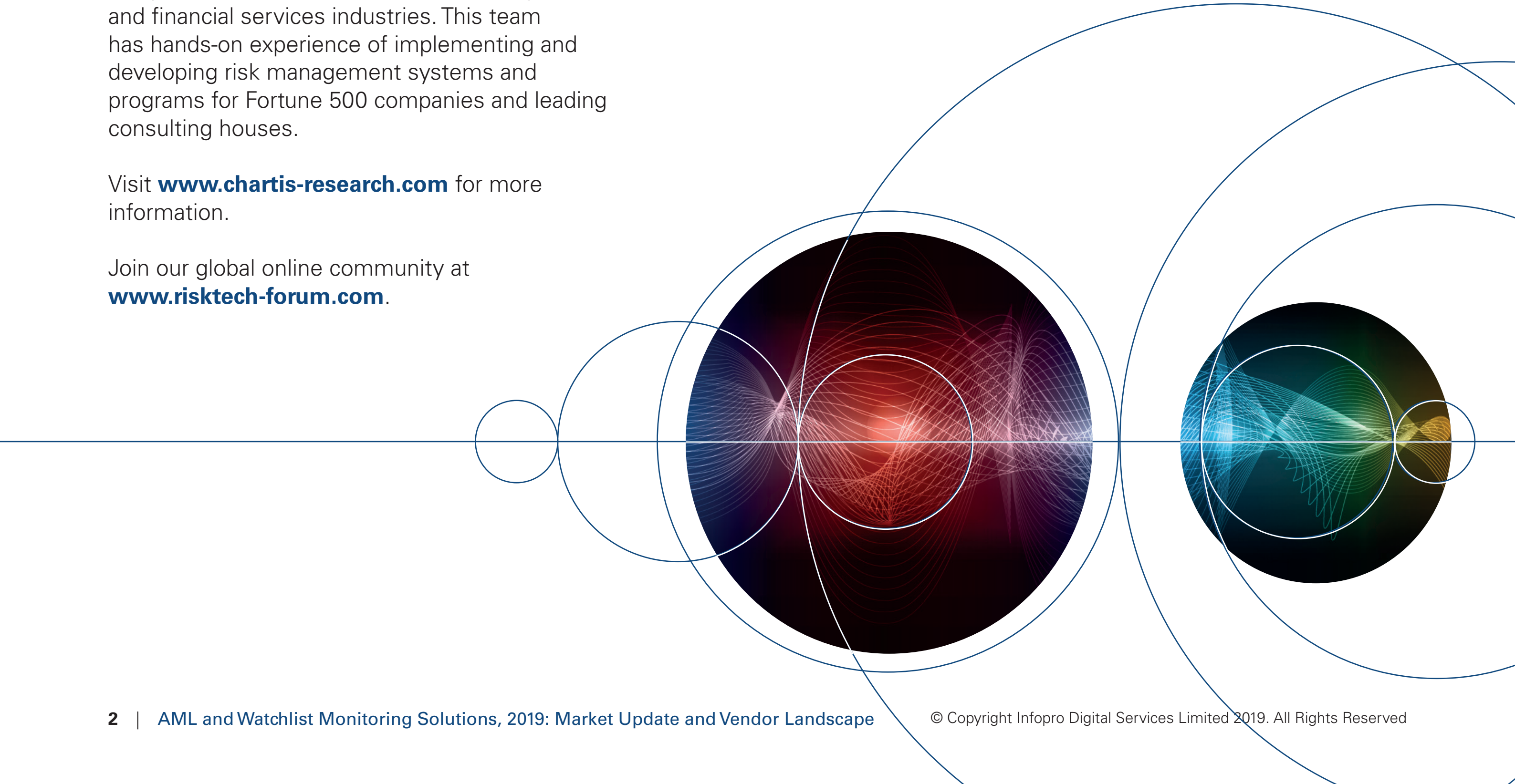


Table of contents

List of figures and tables

1. Executive summary

This is Chartis' first dedicated anti-money laundering (AML) report[1]*. It updates the key trends and dynamics in the market, and provides a snapshot of the vendor landscape.*

Market update

The AML market landscape varies in its maturity and depth – while AML is well-established in western banks, for example, it is less mature in other geographies and industries. Within financial institutions (FIs), AML capabilities increasingly function on a continuum: centralized within specific compliance departments, but also present in other operational areas such as Know Your Customer (KYC) and customer lifecycle management (CLM).

In areas like retail banking where AML is relatively mature, FIs have reached an equilibrium. They are onboarding fewer suspicious customers, and growth in suspicious activity reports (SARs) – the primary AML indicator – has flattened. But these developments have come at the cost of large and hugely inefficient compliance departments, often containing thousands of employees.

FIs now want to reconfigure their existing AML processes to make them more efficient and valuable. But there has also been a shift toward *understanding* and *quantifying* AML solutions, rather than creating ever more complex tools and systems. This has sharpened the focus on model risk management and validation capabilities, to enable FIs to interrogate and authenticate existing models. Vendors and FIs are also considering new ways to express AML information, such as delivering it as a single headline figure (a 'compliance score' similar to a credit score).

As AML use matures in investment and retail banking, it is spreading into other areas, notably trade finance, gambling and the FinTech sector. Trade finance is an especially complex area for AML, with many constraints and a reliance on sometimes limited data that can vary across geographies. Nevertheless, trade-based AML is having a significant business impact on FIs, and is a valuable potential market for new vendors.

Vendor landscape

Packaged solution vendors and data providers remain the backbone of the AML marketplace. But new entrants, such as commercial workflow and advanced analytics vendors, pose a threat, especially to packaged solution vendors. FIs, especially large and complex ones, are looking to establish core case management functionalities with additional components. End-to-end solutions will increasingly be used by smaller firms with less complex data and customer requirements.

While the new players are unlikely to challenge incumbents in their core area of case management, they are increasingly likely to attack the 'edges' of their capabilities, in areas such as transaction monitoring, entity resolution and segmentation analytics.

Finally, as AML moves beyond its core compliance areas, solution vendors are having to consider ancillary sectors where it is relatively immature, such as trade finance, gambling and the burgeoning FinTech sector (with technology companies providing financial services). While these areas offer new opportunities, they also bring their own challenges and impacts for the vendor landscape, in addressing the wide range of firms and requirements they contain.

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 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 providers of AML/watchlist monitoring solutions: Accuity, ACI Worldwide, AML Partners, Arachnys, Ayasdi, BAE Systems, BlackSwan Technologies, Clari5 (by CustomerXPs), EastNets, Fenergo, FICO, FinScan, Fiserv, GBG, idetect, InfrasoftTech, Intellect Design, LexisNexis Risk Solutions, Manipal Group, NICE Actimize, Oracle, Pelican, RDC, Refinitiv, SAS, Silent Eight and Verafin.

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 this research.

[1] *For our previous AML/watchlist monitoring research, see 'Financial Crime Risk Management Systems: Market Update 2017'.*

2. Market update

FIs remained concerned about AML sanctions and fines, and not just for actual breaches. Failure to act on prior warnings can also lead to hefty penalties. In October 2018 Capital One received a $100 million penalty from the Office of the Comptroller of the Currency (OCC) for deficiencies in its AML program, and for failing to comply with an earlier order[2].

The global strength of the dollar means that US regulators – with the potential to deny access to dollar swaps or the SWIFT[3] network (or both) – are among the most feared. Among US financial crime and sanctions monitoring bodies, the New York Department of Financial Services (NYDFS) has been relatively aggressive in penalizing non-US firms. But it is not unique – in March 2018 the Federal Reserve urged the Industrial and Commercial Bank of China (ICBC) to improve its AML controls; two months later it was hit with a fine of $5.3 million from the Financial Industry Regulatory Authority (FINRA)[4].

As we explored in our previous report[5], as part of their AML process FIs must now monitor their correspondents and subsidiaries with the same level of diligence as they use for their primary business lines. Sensitivity to AML compliance has led some FIs to sever many of their correspondent banking relationships, cutting clients and shifting their business focus from global to regional, and to territories where they are comfortable taking on risk.

Against this background, three trends are changing the AML market and vendor landscape:

- As AML software components are embedded in areas of the business outside compliance, FIs are looking for ways to make their AML processes more efficient.
- For risk-averse FIs facing heavy regulatory pressure, using advanced analytics is becoming an area of increasing uncertainty.
- AML requirements and capabilities are moving into adjacent sectors and industries, notably trade finance, gambling, and the FinTech sector.

A drive for efficiency as AML spreads

Traditionally AML has been handled largely by compliance departments, but it is now spreading into other areas of FIs' business. SARs remain a consistent burden for institutions – according to the Financial Crimes Enforcement Network (FinCEN), SARs filings reached a peak of almost 1 million in 2018 – although SARs growth is flattening.

Increasingly, AML system components sit in parts of the business (such as FX trading systems) that are outside compliance departments, which can now generate their own SARs. This shift in technical architecture is part of an effort by FIs to reduce the work the compliance department has to do, and the staff it needs to do it – and to help it deal with the more real-time nature of transactions. This in turn has contributed towards moves to reconfigure pre-existing AML processes, to drive more value from them and/or make them more efficient.

Near-zero risk appetite makes advanced analytics a challenge

For FIs, the success of an AML system is usually measured by the amount of time it saves and its reduction of false positives. Fearing an adverse reaction from regulators, however, FIs are reluctant to lower their SARs levels or try new technology solutions. So false positives remain high and true positives elusive, with attendant business issues, as UK FinTech firm Revolut discovered when it had to turn off an AML system because of its tendency to produce false positives[6].

This situation creates challenges in the use of advanced analytics, and in particular machine learning (ML). The dearth of true positives on which to train the analytics means it is difficult to tune ML models for AML. And explaining the outcomes to regulators and stakeholders can be a challenge in itself. Consequently, there has been a move toward *analyzing* and *understanding* AML analytics and the underlying data – to increase the 'explainability' of these tools rather than their complexity.

[2] **https://www.cnbc.com/2018/10/23/reuters-america-capital-one-bank-fined-100-mln-for-anti-money-laundering-weaknesses.html**
[3] *The Society for Worldwide Interbank Financial Telecommunication.*
[4] **http://www.finra.org/newsroom/2018/finra-fines-icbcfs-53-million-anti-money-laundering-compliance-deficiencies-and-other**
[5] *'Financial Crime Risk Management Systems: Market Update 2017'*
[6] **https://www.pymnts.com/news/digital-banking/2019/revolut-cfo-resign-aml/**

Because FIs prioritize efficiency, they are focusing on quantifying and delivering headline AML information that can be interrogated and sourced, and using techniques such as robotic process automation (RPA) to automate manual processes. While entirely automating the highly sensitive AML process is extremely difficult, configurable, analytics-driven RPA can make case management and workflow much more efficient.

Early RPA projects promised considerable reductions in compliance staff, but FIs may not be able to achieve these – nor, ironically, may they want to. AML is not just a process of catching potential money-launderers and criminals, but of demonstrating a willingness to do so. Regulators may view a reduction in compliance staff as indicative of an unwillingness to address the issue. So successful RPA tends to provide assistance, auto-populating fields during compliance processes, for example.

AML expands into adjacent areas

While FIs in which AML is embedded (such as major retail and investment banks) have been driving for more efficiency, AML capabilities are also spreading into other areas with their own requirements:

- Trade finance.
- Gambling and gaming.
- The FinTech sector.

AML in trade finance

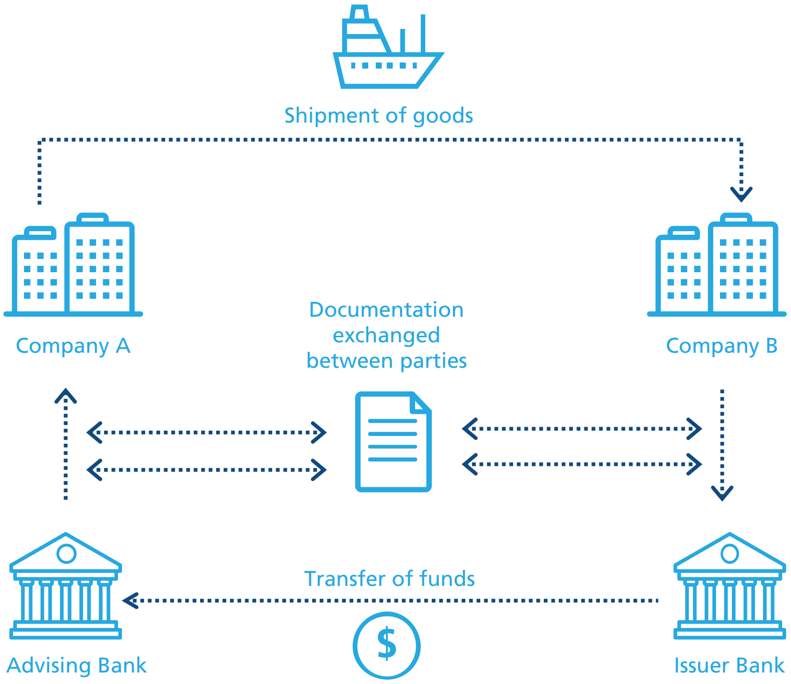
According to the 2017 Global Financial Integrity[7] report, between $1.4 and $2.5 trillion is transacted via illicit trade flows. Trade-based money laundering can be achieved by misrepresenting the price, quantity or quality of imports or exports. Having to keep track of all these factors is a challenge – any of them could be misrepresented to facilitate money laundering, and factors such as price are highly variable, particularly across different geographies.

Trade-based money laundering has a genuine impact on FIs, which lose business if they cannot confirm KYC capabilities with their trading counterparties. Chartis has spoken with banks that have even pulled out of specific countries and regions because they cannot effectively account for trade compliance across their organizations.

Trade finance often involves documentation concerning certain items, such as a description of goods being imported or exported, their quantity, value, weight, customs or tariff code number. This information is shared between the trading institutions and their supporting firms, which shoulder the burden of AML reporting for the transaction (see Figure 1).

To map the information around these trades, FIs require transaction monitoring capabilities that can incorporate this information effectively.

Figure 1: Trade finance flows



Source: Chartis Research

Monitoring trade-based AML also requires complex workflow tools to capture multi-stage processes, and an entity data model system that can capture the surrounding dynamic information (such as prices). So far, in Chartis' opinion, few vendors are providing suitable solutions in this area, creating opportunities for providers with the right offerings.

AML in gambling and gaming

Growth in AML use is less aggressive in the gambling sector than in trade finance, but this area remains of significant interest to vendors. As casinos' customer numbers grow and attention

[7] **https://www.gfintegrity.org/wp-content/uploads/2017/04/GFI-IFF-Report-2017_final.pdf**

from regulators increases, they are improving their Bank Secrecy Act (BSA) and AML compliance programs, especially around reporting and filing SARs.

In recent years, fines issued to gambling and gaming companies for AML-related violations have increased exponentially, and are unlikely to drop significantly, not least because the underlying market is set to expand. In May 2018, the US Supreme Court allowed individual US states – including Nevada, Rhode Island, Pennsylvania, Delaware and New Jersey, although others are likely to be included – to offer sports betting in accordance with their own state statutes and laws[8]. This is likely to expand the power and scope of gaming companies, and increase their exposure to AML-related incidents.

AML and FinTechs

As FinTech firms become more established across the financial services value chain, they look likely to mirror existing FIs in terms of their structure. The advantage in their business models has often been in regulatory arbitrage (using consumer deposits as a largely interest-free source of investment funding, for example)[9]. As they grow in size and regulatory attention increases, these funding methods will disappear and FinTechs will increasingly resemble the institutions they were nominally set to displace.

As a result, their AML requirements are likely to resemble those of incumbent FIs. FinTechs' KYC and AML processes are often relatively immature: many companies often look for high user growth at the possible expense of compliance.

One difference between FinTechs and established FIs is that their AML technology requirements are already fairly clear. In contrast to established FIs, which have had to install third-party AML solutions into pre-existing legacy structures, FinTechs could incorporate AML into their core systems, and will look for vendors with expertise in both approaches. FinTechs' high-volume, low-value business also means that they will typically favor lightweight third-party solutions.

Chartis believes that the market for AML solutions for FinTechs is currently much less lucrative than others in terms of deal size. Nevertheless, it offers an opportunity for vendors to embed their offerings into a new generation of FIs, although the market is crowded. Ultimately, this approach will likely suit vendors that already have significant FinTech or core banking relationships, and which can produce lightweight AML solutions.

[8] **https://www.nbcnews.com/news/us-news/sports-betting-now-legal-several-states-many-others-are-watching-n894211**
[9] *'Big Tech in finance and new challenges for public policy'* - **https://www.bis.org/speeches/sp181205.pdf**

3. Vendor landscape

Many vendors provide AML as part of their solution set, because AML components are increasingly incorporated into a wide range of processes (including operational processes such as KYC and CLM). Incumbent and established providers tend to dominate among specialist AML and sanctions solutions providers, and the combination of analytics challenges and FIs' low risk appetites means that 'trusted' vendors have significant and durable market presence.

As we highlighted in our previous research[10], the incumbents fit broadly into two groups:

- **Packaged solution vendors**. Typically these have powerful case management and workflow capabilities, and they are often ahead of the field in establishing RPA capabilities.

- **Data provision firms** provide sanctions screening and user data, and are often mistakenly assumed to merely provide raw data for the compliance process. But their ability to work with large, proprietary data sets gives them an advantage in live-testing ML and advanced analytics, and in building experienced data science teams.

The market changes outlined in the previous section – especially the **growing challenge of analytics** and **AML's move into other sectors** – are driving changes in the relevant technology. Much of the change in the AML marketplace comes in areas such as the adoption of innovative analytics and model risk management, and the services and technology mixtures of the vendors.

The analytics challenge

A drive for interpretation and explicability

FIs tend to spend on AML solutions in large, discrete chunks, making AML an attractive market for vendors and services firms. However, these firms have often over-promised on their offerings, creating a cycle of replacement and disillusionment, and FIs now want tangible results. Vendors attempting to reduce false positives, for example, will increasingly be asked difficult questions, like 'how?', 'against what benchmark?', 'under what constraints?', and 'across training or live data?'

While the underlying nature of AML and sanctions screening has remained relatively stable, this new approach is encouraging vendors to deliver more value and explicability from AML processes, using techniques like **model risk management**.

But FIs also want more efficiency, and this has been partially enabled by a change in how information is surfaced. Vendors have often looked to their other areas of expertise to provide more innovative forms of scoring. One example is the use of a 'credit scoring'-style methodology to provide a single aggregate AML score to users based on a variety of attributes. In addition, firms with expertise in defined areas such as card fraud have been looking to establish transaction monitoring-based analytics for AML that mirror the kind of results obtained in card fraud.

Segmentation becomes more widespread

Vendors typically move quickly to integrate effective analytics techniques into their solutions. The currently popular analytical technique is segmentation analysis (using topological data analysis or graph analytics). This enables users to divide entities into defined groups based on their behavioral traits. These segments can then be passed to other analytics systems, which typically involve rules-based techniques. Segmentation analysis is provided both by firms that specialize in those techniques (often in partnership with larger vendors) or as a specific module within an enterprise vendor's systems. Increasingly, these analytics cannot be considered a differentiator among vendors, or at least not one as unique as it was a few years ago.

Expansion into new areas

Trade finance

Trade finance is difficult to address because it requires complex entity data models, especially those that can efficiently establish ultimate beneficial owners (UBOs). Analyzing complex documents is a particular issue for players in this space. Transactions can be highly structured, with multi-level payments and even equity financing. The range of data that needs to be integrated and analyzed is broader too, and can come in multiple formats.

[10] *'Financial Crime Risk Management Systems: Market Update 2017'.*

While many vendors are already staking out a space in the trade finance area, there are significant gaps in coverage. So far no single solution (or combination of key components) exists in the market.

Gaming and gambling

Regulatory and organizational complexity in different areas of the gambling sector pose significant challenges for vendors. Different segments have different gaps. Casinos catering to high-net-worth individuals, for example, will need a deep understanding of their clients' political exposure, while online-only gaming requires real-time solutions at the high-performance end of the technology spectrum. So far no single solution covers this sector fully, and client requirements are diverse. Many institutions have already established basic AML processes, but vendors' focus is mainly on analyzing a few large and complex firms.

FinTechs

Recognizing that FinTechs and their budgets are far smaller than those of established FIs, vendors have a tricky 'value versus volume' problem to solve. FinTechs will likely need lightweight systems, and many will focus on integrated KYC rather than vendor-provided solutions. Vendors are often looking to embed themselves early, effectively gambling on whether a firm (or family of firms) will increase its market presence later. At the current time, however, there is still some uncertainty over just how valuable the FinTech AML market is.

Services vs technology provision

Much of FIs' AML expenditure typically goes to services firms, so a question facing many vendors is how to balance services and technology, and how to divide the human elements of their offerings from the technological ones. A firm that provides only technology components, and which relies on partners or third parties to provide services for an AML project, risks missing out on efficiencies and synergies between services and technology (depending on the services teams' familiarity with the technology, for example, or how it can be reconfigured). Conversely, a firm that offers services opens itself up to 'scope creep', and to shouldering the ballooning costs of implementation.

There is no right answer. Vendors can benefit from a technology focus by selling defined packages to produce a consistent, stable revenue stream, or they can combine the efficiencies of services and technology. The most successful vendors are those with clearly defined strategies: defining where and when they are willing to invest, and where exactly they have the services and technology resources to address a given problem. The boundaries continue to blur, and firms on both sides continue to bolster their capabilities.

Vendor overview

Incumbent vendors will continue to dominate the AML market for some time, but packaged vendors face the greater threat from new players. They still have a significant market presence, largely built on their dominance in case management and workflow capabilities, which they will build on with RPA, and by integrating new analytics capabilities such as segmentation analytics. Their main threat comes from advanced analytics and infrastructure firms from neighbouring areas (such as anti-fraud and commercial workflow vendors) targeting the areas they cover.

Data provision vendors are more durable, benefiting from a wide network that can give them an advantage in building data science teams for validation and modelling that can then be repurposed to address data and services. Other firms typically orbit around them, providing either specific analytics capabilities that can be integrated with pre-existing case management functionality or unique AML scoring capabilities.

Vendors looking to establish their AML solutions have several choices. Smaller FIs may wish to invest in a solution that provides integrated headline AML information, while larger FIs may want more complex information, delivered with model validation capabilities and RPA to maximize gains in efficiency. For reliability, they should purchase an incumbent to provide the case management 'heart' of their solution, and establish application programming interface (API) connections to data-provision specialists. They may have to choose whether they supplement these choices with other vendors.

As AML continues to expand into other areas, FinTechs will be looking for lightweight solutions, while gambling and trade finance remain nascent sectors perhaps awaiting a new generation of vendors to solve their challenges.

RiskTech Quadrant® for AML/watchlist monitoring solutions, 2019

Figure 2 illustrates Chartis' view of the vendor landscape for AML/watchlist monitoring solutions. Table 1 lists the Completeness of Offering and Market Potential criteria we used to assess the vendors. Table 2 lists the vendor capabilities in this area.

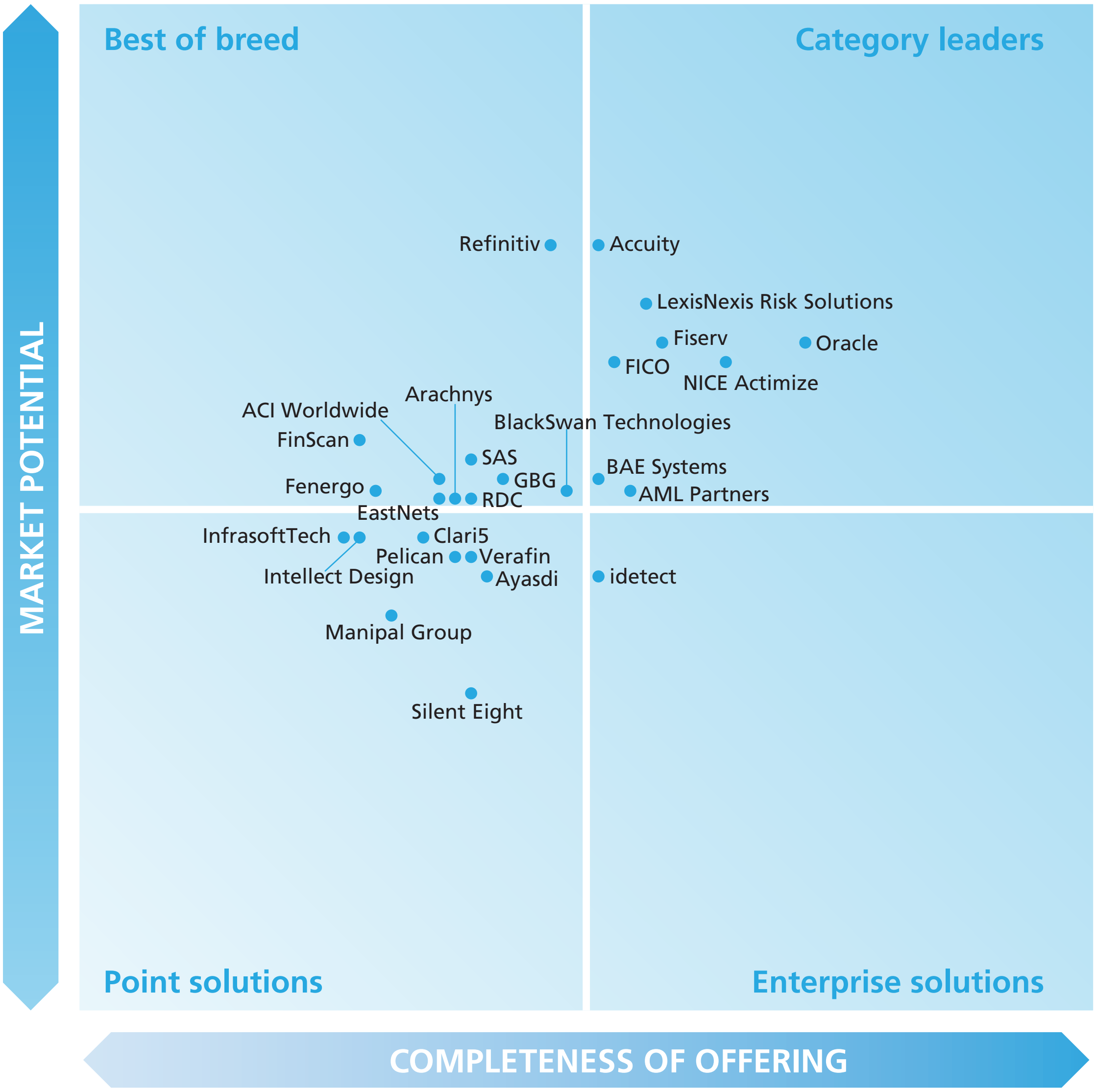
We aim to provide as comprehensive a view of the vendor landscape as possible within the context of our research. Note, however, that not all vendors we approached responded to our requests for briefings, and some declined to participate in this research.

Table 1: Assessment criteria for vendors of AML/watchlist monitoring solutions, 2019

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

Source: Chartis Research

Figure 2: RiskTech Quadrant® for AML/watchlist monitoring solutions, 2019



Source: Chartis Research

Table 2: Vendor capabilities for AML/watchlist monitoring solutions, 2019

	Name and transaction screening capabilities	Breadth of name screening sources offered	Transaction monitoring capabilities	Regulatory compliance reporting and controls	Alert/case management	Advanced analytics	Visualizations and dashboarding
Accuity	***	***	**	**	*	***	**
ACI Worldwide	**	**	**	**	**	**	*
AML Partners	**	**	**	**	***	**	**
Arachnys	*	***	*	**	**	**	**
Ayasdi	**	*	**	*	**	***	***
BAE Systems	**	**	**	**	***	**	**
BlackSwan Technologies	**	**	*	**	**	**	**
Clari5	**	**	**	**	**	**	*
EastNets	***	**	**	**	*	*	**
Fenergo	**	**	*	*	**	**	*
FICO	**	*	**	**	**	***	**
FinScan	**	**	*	**	**	**	*
Fiserv	**	**	**	**	**	**	***
GBG	**	**	**	*	**	**	*
idetect	***	***	**	**	*	**	**
InfrasoftTech	**	**	**	*	*	**	*
Intellect Design	**	**	**	**	*	*	*
LexisNexis Risk Solutions	***	***	**	**	**	**	**
Manipal Group	**	**	**	**	**	*	*
NICE Actimize	**	**	**	***	***	**	**
Oracle	**	**	**	***	***	***	**
Pelican	**	**	***	*	**	**	*

	Name and transaction screening capabilities	Breadth of name screening sources offered	Transaction monitoring capabilities	Regulatory compliance reporting and controls	Alert/case management	Advanced analytics	Visualizations and dashboarding
RDC	**	***	*	**	*	***	*
Refinitiv	*	*	**	**	**	***	**
SAS	*	*	**	**	**	***	**
Silent Eight	**	*	**	*	**	***	**
Verafin	**	**	*	***	***	**	*

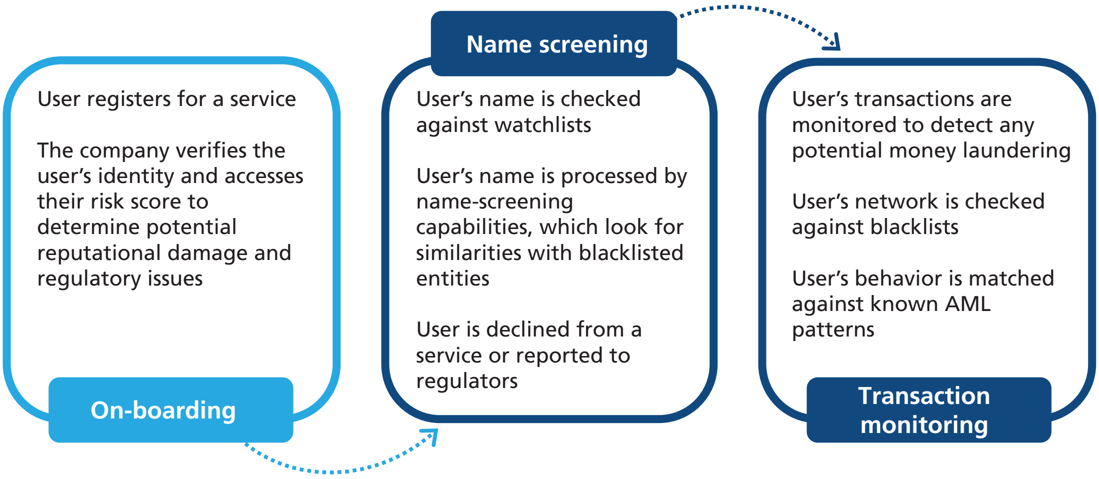
*Key: *** = Core strength/advanced capabilities; ** = Meets industry requirements; * = Partial coverage/component capability.*
Source: Chartis Research

4. Appendix A: Defining AML

Anti-money laundering (AML) refers to all policies and procedures to prevent money laundering, in particular name screening and transaction monitoring. While AML in the more established compliance context tends to be more batch-based, with slower processes, AML solution components are being integrated into other operational processes, and these tend to be more real-time oriented.

- **Name screening**. This starts early in the AML process (see Figure 3). Name information is checked against lists to ensure that an individual is not prohibited from interacting with the FI. This primarily involves sanctions and watchlist screening – in which entities are compared against pre-existing lists of sanctioned entities from bodies such as the Office of Foreign Assets Control (OFAC) and FinCEN – and checks against the FI's internal blacklists. The process uses text matching to compare multiple different spellings or interpretations of names (such as Rob and Robert, for example).
- **Transaction monitoring** aims to detect any suspicious transactions that might be part of a money laundering process, after a user has been on-boarded. It may include unusual behavior or risky entities within the flow of transactions and a user's network.

Figure 3: AML process


User registers for a service
The company verifies the user's identity and accesses their risk score to determine potential reputational damage and regulatory issues
On-boarding
Name screening
User's name is checked against watchlists
User's name is processed by name-screening capabilities, which look for similarities with blacklisted entities
User is declined from a service or reported to regulators
User's transactions are monitored to detect any potential money laundering
User's network is checked against blacklists
User's behavior is matched against known AML patterns
Transaction monitoring

Source: Chartis Research

5. Appendix B: RiskTech Quadrant® methodology

Chartis is a research and advisory firm that provides technology and business advice to the global risk management industry. Chartis provides independent market intelligence regarding market dynamics, regulatory trends, technology trends, best practices, competitive landscapes, market sizes, expenditure priorities, and mergers and acquisitions. Chartis'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.

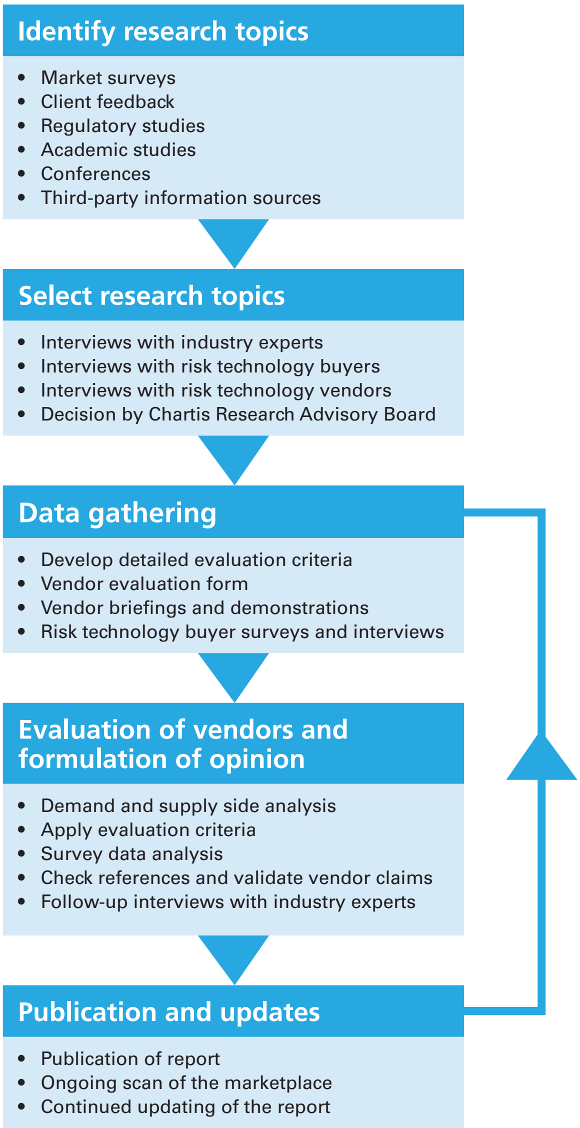
Inclusion in the RiskTech Quadrant®

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 4 below describes the research process.

Figure 4: 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.

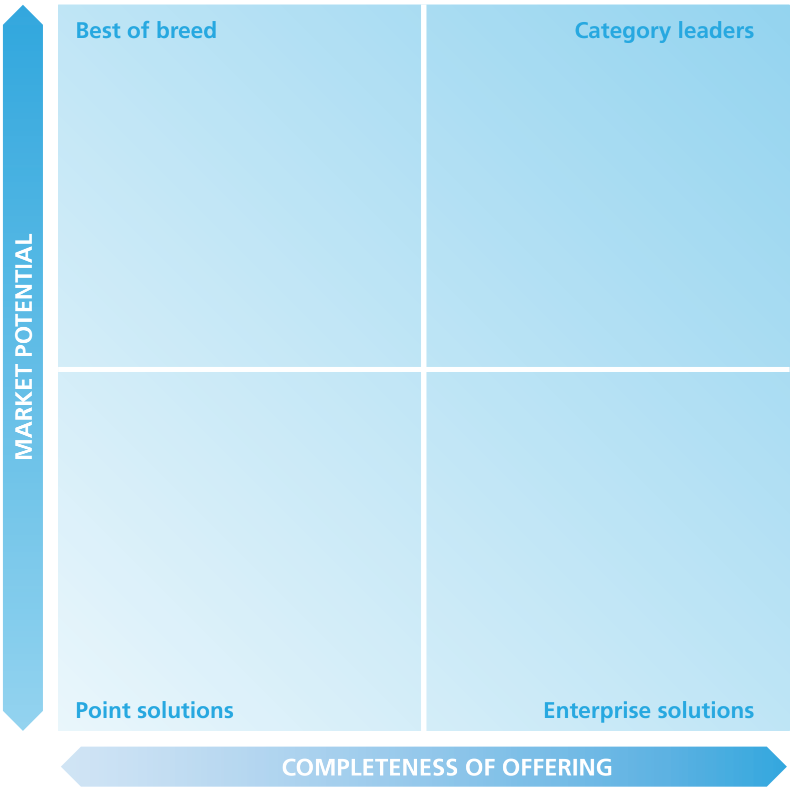
Evaluation criteria

The RiskTech Quadrant® (see Figure 5) evaluates vendors on two key dimensions:

1. Completeness of offering

2. Market potential

Figure 5: 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.

6. How to use research and services from Chartis

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

For risk technology buyers

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

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

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

Our vendor selection services include:

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

For risk technology vendors

Strategy

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

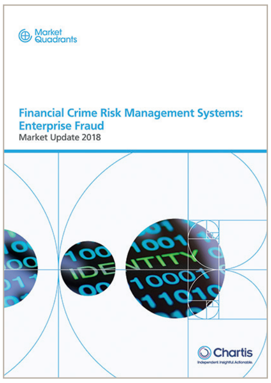
- Market analysis, including market segmentation, market demands, buyer needs, and competitive forces
- Strategy sessions focused on aligning product and company direction based upon analyst data, research, and market intelligence
- Advice on go-to-market positioning, messaging, and lead generation
-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

Thought leadership

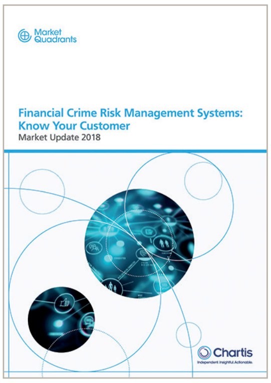
Risk technology vendors can also engage Chartis to provide thought leadership on industry trends in the form of in-person speeches and webinars, as well as custom research and thought-leadership reports. Target audiences and objectives range from internal teams to customer and user conferences. Some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

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

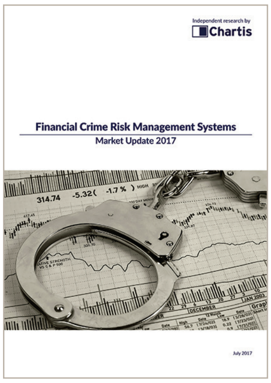
7. Further reading



Financial Crime Risk Management Systems: Enterprise Fraud; Market Update 2018



Financial Crime Risk Management Systems: Know Your Customer; Market Update 2018



Financial Crime Risk Management Systems; Market Update 2017

Market Quadrants
Model validation solutions, 2019
Overview and market landscape
Chartis

Model Validation Solutions, 2019: Overview and Market Landscape

Global Risk IT Expenditure in Financial Services, 2018 Update

RiskTech100 2019

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