Vendor Analysis

Vendor Analysis: SAS

FRAML Solutions, 2023

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**.

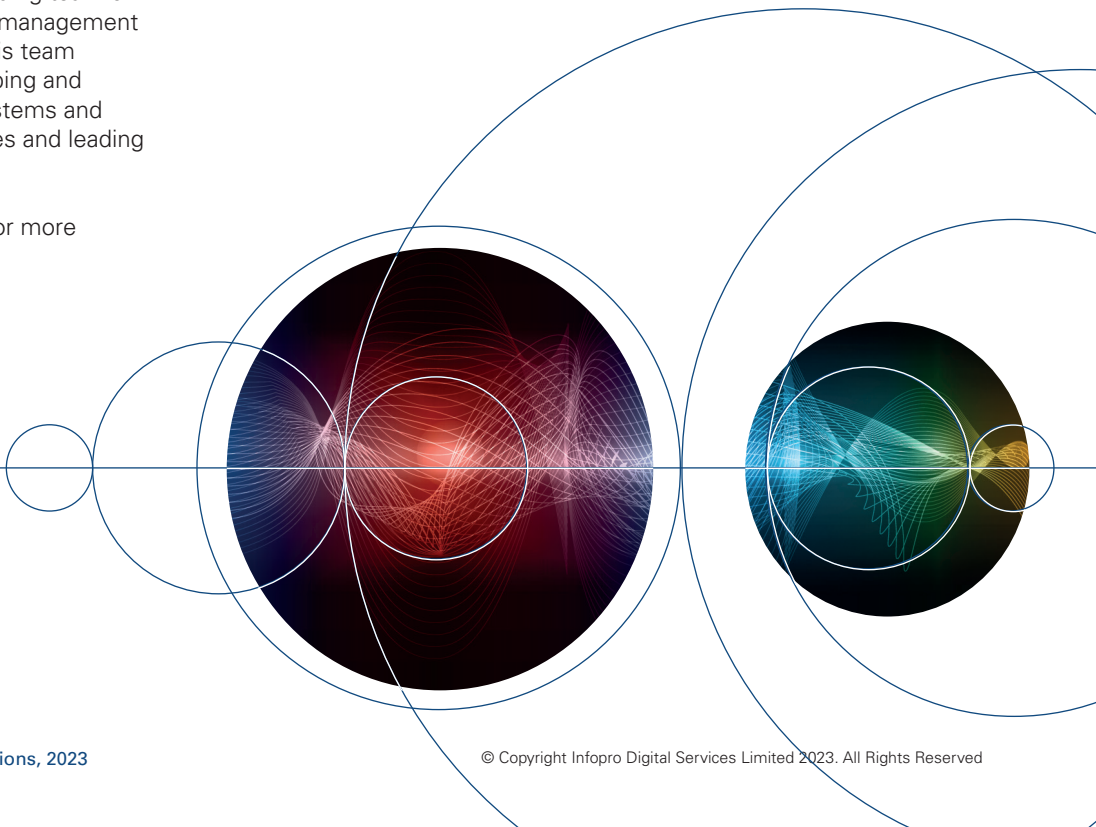


Table of contents

List of figures and tables

1. Report context

This Vendor Analysis is based on the Chartis quadrant report *FRAML Solutions, 2023: Market and Vendor Landscape* (published in November 2023). This section summarizes the key theses in that report; subsequent sections take a detailed look at SAS' quadrant positioning and scoring, and Chartis' underlying opinion and analysis.

Key thesis

As concerns around financial crime escalate, financial institutions and regulators are placing greater emphasis on combined fraud and anti-money laundering (FRAML) solutions. For financial institutions, the benefits of an integrated FRAML platform include enhanced capabilities, improved collaboration, cost-effectiveness and economies of scale. And by merging siloed teams, firms can boost their operational efficiency and optimize their risk management – all of which might help to explain FRAML's growing popularity.

Financial institutions are taking several approaches to FRAML, notably managed services, orchestration and component solutions; some are even restructuring their organizations to align FRAML solutions with increasingly sophisticated customer journeys. Machine learning (ML) tools are also being used to automate many tasks involved in FRAML compliance and solutions, and could revolutionize this space. Vendors, meanwhile, are broadly adopting four categories of approach: managed services; packaged solutions; platform solutions; and data and analytics-focused FRAML.

As a stand-alone packaged solution, FRAML will remain a core part of organizations' drive to fight financial crime in a streamlined and consolidated way. However, it is vital to remember that the requirements of a FRAML process are highly contextual, and can vary according to several factors, including jurisdiction, operating model, size and business line. This makes it difficult to treat FRAML as one distinct approach. Indeed, ultimately, the term 'FRAML' could be misleading, and even obsolete. Although firms can make significant operational gains by combining fraud and AML workflows, what they are actually pursuing goes beyond just these two disciplines. Longer term, firms may want to move toward a real-time view of customer risk that encompasses both event-based risk (such as behavioral and transactional indicators) and stationary risk (such as more conventional Know Your Customer [KYC] risk indicators).

Demand-side takeaways

Fraud and money laundering are often linked crimes. Fraudulent activity may indicate a potential money-laundering risk; risks in both areas often require similar approaches to their detection and mitigation (such as identifying, escalating, managing/blocking and communicating).

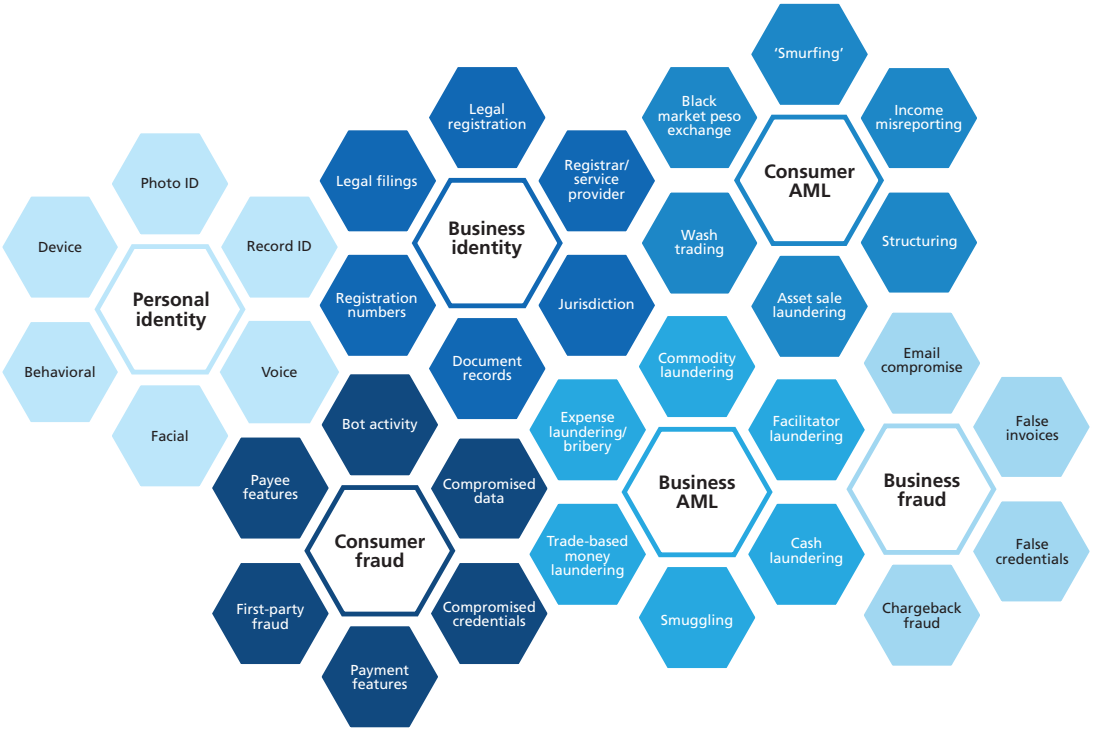
Fraud is typically defined as wrongful/criminal deception for financial and/or personal gain. While fraud comes in many forms, all have the same aim – for their perpetrators to receive a benefit to which they are not entitled. Fraud can also be committed in the pursuit of money laundering – essentially the movement of illicit funds through legitimate businesses to conceal their source. In organizations, approaches to preventing fraud and money laundering are often shared. Traditionally, fraud has been an issue of security, while AML was handled by compliance teams. As criminals do not make this distinction, however, firms have increasingly sought to combine fraud and compliance teams into FRAML operations.

FRAML reflects firms' increasing focus on – and the convergence of – fraud and money laundering detection (see Figure 1), and it highlights the benefits of taking an integrated approach to mitigating and detecting financial crime.

For one, fraud management and AML teams have the following common goals:

- To shield customers and protect organizations from the impacts of financial crime.
- To stay compliant with regulations.

Figure 1: The increasing convergence of fraud and AML



Source: Chartis Research

Trends in the FRAML landscape

Integration approaches

In our research, we are seeing the following approaches to FRAML solution integrations in the marketplace:

- **Organizational restructuring**, which involves the convergence of fraud and AML functions within an organization. This may be to benefit from economies of scale, or to make the system better aligned with an increasingly frictionless customer experience.
- **Managed services**. This option is for banks and financial institutions that lack the resources to build a solution and that require a more 'out-of-the-box' approach.
- **Orchestration of a FRAML platform** with best-of-breed solutions. This option tends to be for organizations that are looking to retain a broad set of vendor options without significant integration.
- **Multiple best-of-breed component solutions** built around a core banking (or similar) platform. This is typically the approach adopted by Tier 1 banks, although many still have separate fraud and AML functions.

The machine learning effect

Real-time detection using ML tools has proved especially useful in detecting financial fraud as it happens, and has greatly empowered fraud-management teams. Indeed, ML is often used to automate many tasks involved in FRAML compliance and solutions.

Supply-side takeaways

Despite the ongoing definition and redefinition of fraud and AML, FRAML as a concept is fairly loosely interpreted – and with good reason. The idea of combining fraud and AML systems has evolved from a workflow approach aimed at standardization into a realization that exploring the flow of criminal activity can help firms detect and prevent it. Banks, FinTechs and other stakeholders (including policymakers) are realizing that by combining views on a number of risk typologies including – but not limited to – fraud and money laundering, they can obtain a broader view of risk and connect the dots between various interlinked activities.

With this in mind, we have found that the requirements of a FRAML process, whichever interpretation an organization uses, is highly contextual, and can vary according to (among other factors) an organization's jurisdiction, operating model, size and business line. This makes it difficult to treat FRAML as one distinct approach.

Rather, we are seeing different approaches to managing FRAML (what could be termed 'FRAML+'), many of which go beyond a relatively straightforward view of combined fraud and AML systems. We group these approaches into four broad categories: managed services; packaged solutions; platform solutions; and data and analytics-focused FRAML.

So what conclusion can be drawn about FRAML? As a stand-alone packaged solution, it will remain a core part of organizations' drive to fight financial crime in a streamlined and consolidated way. As the complexity and difficulties involved in detecting financial crime grow, however, so does the need for a combined, enriched and more robust view of risk. The direction of travel is very firmly toward the amalgamation of interconnected risk typologies, beyond just fraud and AML. What form that particular approach will take will depend on many factors, including practicality. What is clear, though, is that whatever form of amalgamation FRAML takes, it will need to be flexible, scalable and able to adapt to ever-changing financial crime.

2. Quadrant context

Introducing the Chartis RiskTech Quadrant®

This section of the report contains:

- The Chartis RiskTech Quadrant® for FRAML Solutions, 2023.
- An examination of SAS' positioning and its scores as part of Chartis' analysis.
- A consideration of how the quadrant reflects the broader vendor landscape.

Summary information

What does the Chartis quadrant show?

Chartis' RiskTech Quadrant® uses a comprehensive methodology that involves 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 option as the best FRAML solution; rather it has a sophisticated ranking methodology to explain which solutions are best for specific buyers, depending on their implementation strategies.

The RiskTech Quadrant® is a proprietary methodology developed specifically for the risk technology marketplace that takes into account vendors' product, technology and organizational capabilities. Section 4 of this report sets out the generic methodology and criteria used for the RiskTech Quadrant®.

How are quadrants used by technology buyers?

Chartis' RiskTech Quadrant® and FinTech Quadrant™ provide a view of the vendor landscape in a specific area of risk, financial and/or regulatory technology. We monitor the market to identify the strengths and weaknesses of different solutions and track the post-sales performance of companies selling and implementing these systems. Users and buyers can consult the quadrants as part of their wider research when considering the most appropriate solution for their needs.

Note, however, that Chartis does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Chartis' publications consist of the opinions of its research analysts and should not be construed as statements of fact.

How are quadrants used by technology vendors?

Technology vendors can use Chartis' quadrants to achieve several goals:

- Gain an independent analysis and view of the provider landscape in a specific area of risk, financial and/or regulatory technology.
- Assess their capabilities and market positioning against their competitors and other players in the space.
- Enhance their positioning with actual and potential clients and develop their go-to-market strategies.

In addition, Chartis' Vendor Analysis reports, like this one, offer detailed insight into specific vendors and their capabilities, with further analysis of their quadrant positioning and scoring.

Chartis Research RiskTech Quadrant® for FRAML Solutions, 2023

Figure 2 illustrates Chartis' view of the FRAML solutions vendor landscape, highlighting SAS' position.

Quadrant dynamics

Vendor positioning in context – completeness of offering

SAS achieved category leader status for FRAML solutions largely because it offers in-depth analysis capabilities across all stages of the analytics lifecycle, from data management to discovery to the deployment of AI into production. By monitoring individuals and entities with constantly improving data within a FinCrime framework, users can make more informed decisions along the whole customer lifecycle.

SAS' FRAML solution provides strong capabilities in almost every area. Its high rating for its packaging and deployment integration capabilities

Figure 2: RiskTech Quadrant® for FRAML solutions, 2023

Source: Chartis Research

reflects how it provides clients with a range of deployment options to fit their FRAML needs, from managed service applications (both on-premise and via the cloud) to client-managed cloud deployments. Clients may choose to take a modular approach to address their most pressing concerns or take advantage of the offering's full end-to-end solution capabilities.

Other notable capabilities offered by SAS' FRAML solution are data management and analytics, and a sophisticated user interface. By simplifying data integration, the solution enables firms to combine all internal, external and third-party data – including structured and unstructured data, text, documents and images – to create better predictive models to suit their particular requirements. By combining this data with SAS' hybrid analytical approach, which uses multiple techniques (including automated business rules, predictive modeling, text mining, exception reporting and network link analysis), firms can spot more suspicious activity with greater accuracy. The SAS engine employs embedded artificial intelligence (AI) and ML techniques, combined with traditional detection methods, to process all data in real time or batch, to help firms detect more fraud and reduce false positives.

Chartis' rating for SAS' FRAML solution's flexibility, scalability and overall orchestration was particularly strong, reflecting the company's self-service capabilities. These intelligently prioritize alerts for triage, investigation and disposition. The solution

also gives firms the flexibility to scale as they change and respond to new fraud threats. As workflows evolve and the technology is able to process 100% of transactions in real-time while generating fewer false positives, firms can provide a better customer experience while detecting more instances of fraud. These capabilities are reinforced by SAS' architecture, as it covers firms' broadening requirements in the areas of fraud and AML.

Table 1 shows Chartis' rankings for SAS' coverage against each of the completeness of offering criteria.

Vendor positioning in context – market potential

SAS' position as a category leader in the Chartis RiskTech Quadrant® reflects how its FRAML solutions have become established as leading fraud and AML service offerings. Robust ratings for customer satisfaction and market penetration reflect the company's large client base, which comprises a variety of firms, including financial services companies and technology organizations.

SAS' high ratings for growth strategy and financials reflect increasing demand for its services. As a long-time leader in analytics, SAS has a strong global market presence, aligned with extensive experience in financial crime solutions, and an established knowledge of organizational issues. To keep up with expanding demand, SAS has widened its areas of focus, taking advantage of its global workforce.

Table 2 shows Chartis' rankings for SAS' coverage against each of the market potential criteria.

Table 1: Completeness of offering – SAS (FRAML solutions, 2023)

Completeness of offering criterion	Coverage
Packaging	High
Deployment integration	High
Data management	High
Flexibility and scalability	High
Orchestration	High
Analytics and UI	High

Source: Chartis Research

Table 2: Market potential – SAS (FRAML solutions, 2023)

Market potential criterion	Coverage
Customer satisfaction	Medium
Market penetration	High
Growth strategy	High
Financials	High

Source: Chartis Research

3. Vendor context

Overview of relevant solutions/ capabilities

Table 3 provides a summary of the vendor and its solutions.

SAS' fraud and financial crime solutions are built on a common technology architecture that can be deployed to address the risks of both fraud and money laundering/terrorism financing. Figure 3 on page 11 illustrates its primary functional components.

Inherent in SAS' fraud and financial crime solutions is SAS' intellectual property for recommended data sources, data mapping and the creation of profiles or signatures. As part of the SAS® Viya® 4 cloud-native architecture, the solution is designed to interact with and improve the governance of third-party data sources and programming languages (including R, Python and Lua).

Table 3: SAS – company information

Company	SAS
Headquarters	Cary, NC, US
Other offices	SAS has offices in 56 countries worldwide.
Description	SAS, one of the largest privately held software companies in the world, is a provider of AI and advanced analytics tools. Used by 91 of the top 100 companies in the global Fortune 500, SAS provides software and services to customers around the world. SAS has evolved its fraud and financial crime solutions since the introduction of SAS® Anti-Money Laundering software in 2002. SAS' fraud and financial crime clients range from global systemically important banks (G-SIBs) that rely on SAS solutions for real-time fraud interdiction, to small and medium-sized institutions that use SAS to comply with money-laundering regulations.
Solution	SAS' fraud and financial crime solutions are built on a common SAS Decisioning Architecture, which provides a consistent technology stack that has been refactored for cloud-native deployment. The Decisioning Architecture is built on orchestration and industry-standard application programming interfaces (APIs) so it can ingest data into its transaction monitoring environment. The monitoring engine supports Boolean and advanced ML strategies that can be deployed in real time, near time or batch. The alert and case management tools are based on open-source business process management (BPM) standards and allow firms to automate triage decisions as necessary. In support of closed-loop self-learning and reporting, the Decision Architecture captures outcomes for reporting and the dynamic refresh of signatures.

Source: SAS

SAS Business Orchestration Services

These manage the asynchronous communication between external data and inputs and outgoing messages (e.g., step-up authentication). The tool accelerates the time to value for supplying data to SAS' landing specifications. SAS has written APIs for more than 20 popular data providers, which deliver intelligence on device reputation, biometric scores, document verification, sanctioned entities and adverse media.

SAS Anti-Money Laundering has a highly scalable behavioral monitoring system that features out-of-the-box (OOTB) scenarios for cash, wire, correspondent banking and anomaly detection. The system has been enhanced to support behavioral segmentation strategies and advanced alert scoring. Many clients use advanced scoring logic to automate the triage of alerts for investigation. SAS' new case management tool is highly configurable, and can support a wide range of financial crime investigations. The tool also supports elastic search and provides dynamic link analysis as a standard OOTB feature.

Beginning with the SAS Viya 4 release, SAS Customer Due Diligence will be included with SAS Anti-Money Laundering software, so that firms can have more tightly integrated scoring between KYC measures and actual behavior. The event-based triggering of enhanced due diligence reviews enables firms to deploy perpetual KYC.

SAS Fraud Decisioning will represent an evolution of SAS Fraud Management software. The software includes an OOTB library of fraud rules, as well as the ability to deploy custom SAS models, consortium SAS models, and open-source models (such as those using Python).

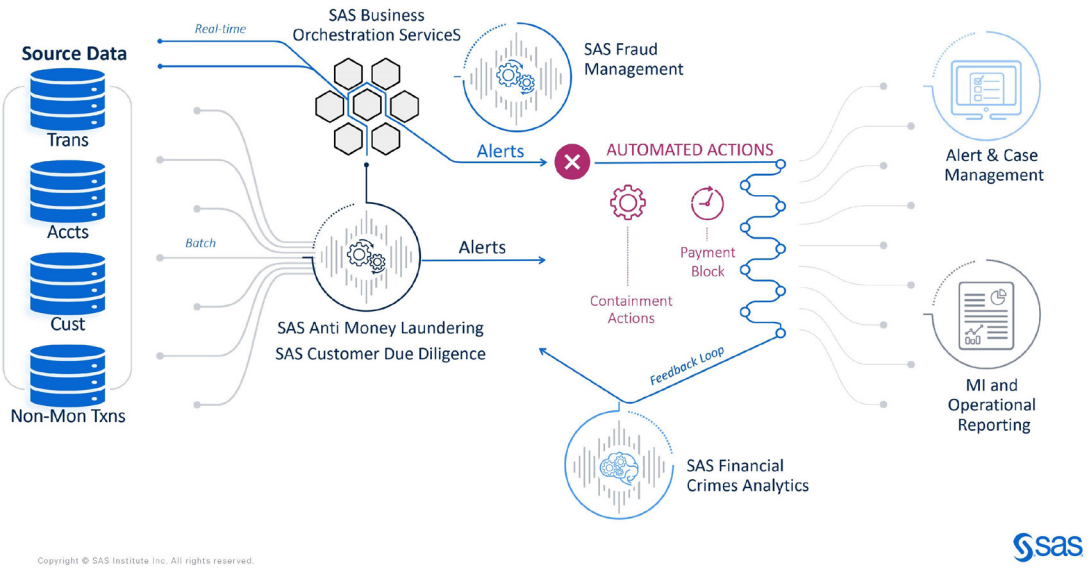
Once events have triggered a review or investigation, work items are persisted in SAS' alert and case management tool. Screens have been configured for specific types of activities (such as fraud alert reviews, AML investigations, enhanced due diligence, or manual case entries). Clients can simply modify screens and workflow via a drag and drop administrative interface.

Many SAS clients leverage the 'Design Time' Financial Crimes Analytics capabilities found in SAS' award-winning ML tools. SAS supports the entire AI lifecycle, from data acquisition to champion-challenger design, as well as the testing of strategies through to deployment.

Vendor leading practices

SAS is a leader in AI/ML, and has more than 20 years' experience of deploying fraud and financial crime solutions for global clients. It has a vast amount of institutional knowledge that varies from fraud to compliance disciplines. SAS' Risk, Fraud and Compliance Solutions team understands not only the business requirements for risk management, but also the steps required to satisfy model governance concerns – all of which are top of mind in the deployment of AI.

Figure 3: SAS' fraud/FinCrime technology architecture



Source: SAS

4. Methodology

Overview

Chartis is a research and advisory firm that provides technology and business advice to the global financial services 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® and FinTech Quadrant™ reports are written by experienced analysts with hands-on experience of selecting, developing and implementing financial technology solutions for a variety of international companies in a range of industries, including banking, insurance and capital markets. The findings and analyses in our quadrant reports reflect our analysts' considered opinions, along with research into market trends, participants, expenditure patterns and best practices.

Chartis seeks to include RiskTech and FinTech vendors that have a significant presence in a target market. The significance may be due to market penetration (e.g., a large client base) or innovative solutions. Chartis uses detailed vendor evaluation forms and briefing sessions to collect information about each vendor. If a vendor chooses not to respond to a request for information, Chartis may still include the vendor in the report. Should this happen, Chartis will base its opinion on direct data collated from technology buyers and users, and from publicly available sources.

Chartis' research clients include leading financial services firms and Fortune 500 companies, leading consulting firms and financial technology vendors. The vendors evaluated in our quadrant reports can be Chartis clients or firms with whom Chartis has no relationship.

Chartis evaluates all vendors using consistent and objective criteria, regardless of whether they are Chartis clients. Chartis does not give preference to its own clients and does not request compensation for inclusion in a quadrant report, nor can vendors influence Chartis' opinion.

Briefing process

We conduct face-to-face and/or web-based briefings with each vendor.[1] During these sessions, Chartis experts ask in-depth, challenging questions to establish the real strengths and weaknesses of each vendor. Vendors provide Chartis with:

- A business update – an overview of solution sales and client satisfaction.
- A product update – an overview of relevant solutions and R&D roadmaps.
- A product demonstration – key differentiators of their solutions relative to those of their competitors.

In addition to briefings, Chartis uses other third-party sources of data, such as conferences, academic and regulatory studies, and publicly available information.

Evaluation criteria

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. The specific criteria used for FRAML solutions are shown in Table 4.

Table 4: Evaluation criteria for Chartis' FRAML solutions, 2023 report

Completeness of offering	Market potential
Packaging	Customer satisfaction
Deployment integration	Market penetration
Data management	Growth strategy
Flexibility and scalability	Business model
Orchestration	Financials
Analytics and UI	

Source: Chartis Research

[1] *Note that vendors do not always respond to requests for briefings; they may also choose not to participate in the briefings for a particular report.*

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 can vary 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 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 and 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 their 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 construction process

Chartis constructs its quadrants after assigning scores to vendors for each component of the completeness of offering and market potential criteria. By aggregating these values, we produce total scores for each vendor on both axes, which are used to place the vendor on the quadrant.

Definition of quadrant boxes

Chartis' quadrant reports do not simply describe one technology option as the best solution in a particular area. Our ranking methodology is designed to highlight which solutions are best for specific buyers, depending on the technology they need and the implementation strategy they plan to adopt. Vendors that appear in each quadrant have characteristics and strengths that make them especially suited to that category and, by extension, to particular users' needs.

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 business intelligence (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.
- Because of their focused functionality, best-of-breed solutions will often be packaged together as part of a comprehensive enterprise risk technology architecture, co-existing with other solutions.

Enterprise solutions

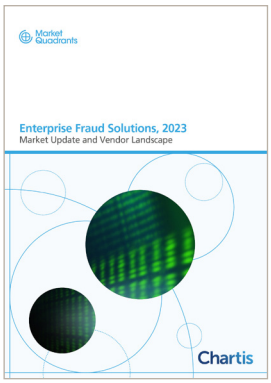
- Enterprise solution providers typically offer risk management technology platforms, combining functionally rich risk applications with comprehensive data management, analytics and business intelligence.
- A key differentiator in this category is the openness and flexibility of the technology architecture 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.
- They 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.
- They typically benefit from strong brand awareness, a global reach and strong alliance strategies with leading consulting firms and systems integrators.

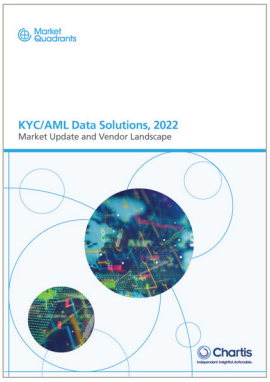
Further reading

FRAML Solutions, 2023: Market and Vendor Landscape

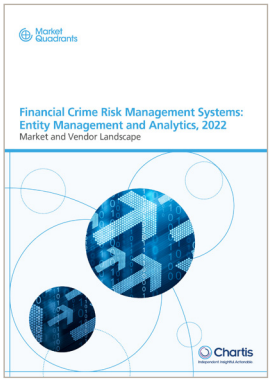


Enterprise Fraud Solutions, 2023: Market Update and Vendor Landscape

KYC Data and Solutions, 2023: Market Update and Vendor Landscape



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



Financial Crime Risk Management Systems: Entity Management and Analytics, 2022; Market and Vendor Landscape

RiskTech100 2024

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