Vendor Analysis

Chartis

Vendor Analysis: SAS

AML Transaction Monitoring Solutions, 2024

Table of contents

List of figures and tables

1. Report context

This Vendor Analysis is based on the Chartis quadrant report **AML Transaction Monitoring Solutions, 2024: Quadrant Update** (published in October 2024). This section summarizes the key theses in that report; subsequent sections take a detailed look at SAS's quadrant positioning and scoring, and Chartis' underlying opinion and analysis.

Key thesis

The global anti-money laundering (AML) ecosystem is changing at a rapid pace. Since Chartis last covered this space less than 12 months ago, we have seen accelerators in the fight against money laundering. A further surge of regulation and supervision is tightening the need for clearer and more connected AML controls. Several factors are the result of a changed perception of the impact of money laundering on the global economy, stemming from more complex and connected criminal and illicit activity. These include the formation of the European Union's Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA), the introduction of the fourth Anti-Money Laundering Directive (AMLD4) in the EU, the now-notorious 'Dear CEO' letter published by the UK's Financial Conduct Authority and the renewed AML/CFT Act in Singapore.

Money laundering and such related areas as terrorist financing and human trafficking are no longer solely the concern of global systemically important banks and law enforcement. Now they are a worry for any organization in the global financial ecosystem, and indeed for society as a whole. In addition, there has been a shift from purely identifying money laundering transactions to assessing money laundering threats across the value chain (including supply chain and customer networks).

Macro- and microeconomic factors, as well as advances in technology, are driving a surge in demand for compliance solutions among financial institutions and corporations. In addition, the market for these solutions is broadening as less regulated industries begin to prioritize robust AML transaction monitoring systems. Buy-side firms – particularly in investment banking and capital markets – have become buyers of extensive transaction monitoring capabilities.

In addition, financial crime compliance and mitigation are no longer solely compliance obligations: they are evolving into strategic operational imperatives. Banks and financial institutions are increasingly recognizing that the risks associated with financial crime extend far beyond regulatory non-compliance. The Wolfsberg Group specifically outlines the need to establish a risk-based set of controls.

Anti-financial crime strategies are now being integrated into broader risk programs to address a range of challenges, including:

- Counterparty risk stemming from involvement in illicit activities.
- Reputational damage linked to money laundering scandals.
- Emerging environmental, social and governance (ESG) risks associated with the ethical implications of financial crime.
- Traditional financial losses due to fraud and asset seizures.

As new industries have emerged, and as the focus has shifted within AML transaction monitoring compliance, the demand for regulatory compliance, operational efficiency, scalability and 'platformization' has grown. All these capabilities are seemingly being prioritized across the AML transaction monitoring landscape.

Financial institutions and payment service providers (PSPs) require varying types of AML transaction monitoring solutions, depending on the size and complexity of the institution or geographical demands, and this has caused the mix of vendor approaches to widen. Transaction monitoring is a relatively mature market with several established players, but we are seeing a strong emergence of newcomers aiming

to disrupt the market with nimble, flexible and often easily accessible solutions. Established vendors are responding by leveraging their heritage and expertise, especially in complex scenarios, and focusing on adding flexibility and scalability to their technology. The market now comprises a finely balanced blend of transaction monitoring solutions, from on-premises to cloud-based, simple to complex and component to enterprise-wide offerings.

Core system providers traditionally have been slow to innovate in the AML landscape – until recently. This is the result of several factors, including the complexity of core systems, the need for backward compatibility and the cost of innovation. Several component players are offering solution functionality to plug the gaps in the AML capabilities of core systems; these firms are typically more innovative than core system vendors.

This year, however, we are seeing the major incumbents invest heavily in advanced analytics capabilities and generative artificial intelligence (GenAI). Some firms have invested extensively in machine learning (ML), deep learning (DL) and GenAI, while others are developing their link analysis capabilities.

- **Pre-built risk typology modeling**. Many vendors offer prepackaged ML models that address specific requirements within a workflow, such as classifying transaction activity. These models, typically developed based on extensive data analysis and industry expertise, provide a foundation for detecting potential money laundering and terrorist financing schemes. While this is a classic strategy of core providers, some component solution vendors also compete in this space.

- **GenAI**. GenAI is by no means designed to replace human analysts and investigators, but can improve efficiency by working alongside and supporting them. From pattern recognition, anomaly detection and risk assessment and scoring to automated case and narrative generation (among other things), GenAI is proving to be powerful in automating and co-piloting an analyst's tasks. Nevertheless, GenAI is a relatively new and developing technology, and its use in AML is evolving. Given its significant potential benefits, however, we can expect to see widespread adoption of this technology in the coming years.

- **Link analysis and knowledge graphs**. Link analysis enables end users to identify complex relationships and patterns within large datasets by mapping connections between entities and capturing semantic meaning. These techniques provide a more comprehensive view of potentially suspicious activity, identifying key entities and third parties and their relationship connections.

Successful players often provide ML and DL anomaly detection, a powerful tool that can be used to identify suspicious activity that is difficult to detect through such traditional transaction monitoring methods as core typology-based solutions. ML and DL can be used in a variety of ways within transaction monitoring to improve the solution's accuracy and efficiency, including anomaly detection, transaction clustering, behavioral analytics and false positive reductions.

Demand-side takeaways

The pace of regulatory fines has surged, with an increase of approximately one-third in the value of fines globally in H1 2024 compared to H1 2023. The most substantial enforcement efforts have been observed within AML, with an outstanding increase of ~87% (~$113 million). Penalties for breaches related to transaction monitoring and suspicious activity reports (SARs) have witnessed an equally staggering rise in the past six months, surging to ~$30 million from ~$6 million, or ~400%. Moreover, in the run-up to this report, and highlighting the importance of automation in transaction monitoring, the Department of Justice and the Financial Crimes Enforcement Network (FinCEN) imposed a landmark fine of more than $3 billion for serious breaches of AML controls, citing gaps in transaction monitoring and a failure to file SARs. This has launched AML and transaction monitoring into the spotlight once again, highlighting the proactive role that the financial sector must play in preventing the facilitation of criminal activity. The global surge in AML transaction monitoring and SAR reporting fines can be attributed to the following key factors:

- **Increased regulatory scrutiny**. As regulatory bodies worldwide have intensified their focus on AML and counterterrorist financing (CTF) compliance, they have been conducting more frequent and thorough investigations. This heightened scrutiny has led to a higher likelihood of identifying and penalizing non-compliant institutions.

- **Increased regulatory fines**. Regulators globally have been imposing increasingly substantial fines for AML violations, with some notable cases in 2024. These have served as a strong deterrent and a message that noncompliance will not be tolerated.

- **Evolving money laundering techniques**. Money launderers constantly adapt their techniques to evade detection. This necessitates continuous updates to AML systems and procedures. Failure to keep pace with these evolving methods can result in violations and subsequent fines. According to our research, 2–5% of the world's GDP is laundered every year, which equates to approximately $1.75 trillion to $4.5 trillion of illicit funds flowing through the global financial system.

- **Increased complexity of financial transactions**. The growing complexity of financial transactions, including the rise of digital assets, cryptocurrency and crypto wallets, and cross-border payments, as well as near-real-time payments (e.g., FX), has made it more challenging for firms to monitor for suspicious activity effectively. This increased complexity can contribute to unintentional violations and subsequent penalties.

Arguably, the combination of stricter regulatory oversight and increased fine amounts, evolving money laundering tactics and the increasing complexity of financial transactions has contributed to the tightening of AML oversight.

More firms are using AML transaction monitoring solutions than ever before. While the financial services industry has been the pioneer in AML compliance, the trend is toward widespread use of transaction monitoring systems across various sectors, notably within capital markets, residential real estate, nonprofit organizations and the gaming industry. The more widespread use of transaction monitoring solutions is based on the following key factors:

- **Evolving regulatory landscape**. Regulatory bodies have become increasingly stringent in their requirements for AML and CTF compliance, demanding more sophisticated monitoring tools.

- **Technological advances**. The development of AI and GenAI, ML and DL, and Big Data analytics has enabled the creation of more powerful and accurate transaction monitoring systems.

- **The impact of fraud on AML**. The growing threat of cybercrime and fraud, especially with such typologies as money mules, has highlighted the need for robust transaction monitoring systems to understand – and cut – the link between funds stolen through fraud and the ability to launder those funds.

- **Cybersecurity control frameworks**. These frameworks are increasingly adopting financial crime controls, with the Financial Action Task Force (FATF) emphasizing the distinction between cybersecurity controls within the broader category of data security.

Supply-side takeaways

The AML transaction monitoring landscape in 2024 is marked by a continued emphasis on technological advances and regulatory compliance. As financial institutions grapple with increasing regulatory scrutiny and the evolving tactics of money launderers, the demand for sophisticated monitoring solutions has never been higher.

The diversity of vendor approaches has increased as smaller financial institutions have begun to require advanced transaction monitoring capabilities, often as out-of-the-box solutions focused primarily on basic alerts and typology-based monitoring. More complex and mature institutions require sophisticated solutions that include advanced analytics, data consortiums and workflow management. As effective data integration becomes more and more essential for managing complex typologies extending beyond standard transaction anomaly detection and rules, such as those associated with mules, advanced analytics will play a crucial role in the process.

The technology footprint of these vendors has also expanded, as firms look to build out such capabilities as link analysis and GenAI. Solution providers have also been required to absorb a plethora of information, including transactional and customer data, to build out analytical views of customers and their potentially suspicious activities.

2. Quadrant context

Introducing the Chartis RiskTech Quadrant®

This section of the report contains:

- The Chartis RiskTech Quadrant® for AML transaction monitoring solutions, 2024.
- An examination of SAS's 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 AML transaction monitoring 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 considers 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 AML transaction monitoring solutions, 2024

Figure 1 illustrates Chartis' view of the vendor landscape for AML transaction monitoring solutions, highlighting SAS's position.

Figure 1: RiskTech Quadrant® for AML transaction monitoring solutions, 2024

Source: Chartis Research

Quadrant dynamics

General quadrant takeaways

Complexity and diversity have been two key drivers in the 2024 AML transaction monitoring quadrant. Firms that have tended to score higher on completeness of offering have invested heavily in more complex analytical modeling and workflow management capabilities, with a focus on unifying data on transaction and customer information. This includes monitoring customer behavior, analyzing metadata and providing a more comprehensive view of the activity.

Vendors have used several different approaches, but those in the far right of the category leader segment have typically been using quantitative transaction monitoring capabilities, a more data-driven

approach that integrates a broad set of data, from identification and verification (ID&V) and fraud signals to KYC data and adverse media. Of course, there is growing use of ML and AI to reduce false positives and generate alerts. Increasingly, low-code/no-code reconfigurability is viewed as table stakes, as are platformization and application programming interface (API) integrations with third parties to give financial institutions a centralized way to access data and functionality from all AML measures.

Many leading vendors have significantly diversified their client base, as transaction monitoring solutions have become a significant concern for more than just banks and FinTechs. Buy-side firms have contributed to the growth of some of the key players in this space. However, their significant foothold in primary markets continues to provide many legacy vendors with a strong, durable market presence.

As a mature and rapidly growing sector, the transaction monitoring market is extremely competitive. The maturity and breadth of the market is reflected in the number of category leaders in our quadrant that occupy leadership positions in several significant market sectors. Chartis believes that this fragmentation and positioning will intensify in the next 12 months, driven by transaction monitoring solutions that apply to specific use cases.

Overall, in our view, the market can be broken down into several clusters, even within the category leader segment:

- Global or multi-region category leaders that occupy many large segments, with functionality tailored to multiple use cases and a proven track record in supporting them (in, for example, Tier 1 banks, FinTechs and the retail and wealth sectors).
- Category leaders that occupy and lead in a large and growing market segment or stage in the TMS lifecycle (specialists in a particular vertical or region, for example).
- Category leaders that are emerging as strong contenders, gaining significant traction but without having yet found a defined niche.
- Enterprise vendors with the appropriate tech stack for multi-use case or vertical specialisms, which are growing in their respective markets but have yet to reach full maturity.
- Point solution and best-of-breed vendors that excel in certain use cases or stages in the TMS lifecycle.

Compared with the 2023 iteration, our 2024 transaction monitoring report presents an expanded view of the market and includes vendors that offer a different approach to transaction monitoring, focusing on analytics, platforms, automation or alert enrichment.

Winning vendors in this space understand the value that their customers seek, whether in integrating data pertinent to a specific region, providing a user interface that is customized to individual use cases or focusing on TMS investigations in customer issues. Looking ahead, this specialization in one or more use cases will prove a winning strategy.

Vendor positioning in context – completeness of offering

SAS's AML transaction monitoring solutions provide strong capabilities across the AML cycle, reflected in its high ratings across all completeness of offering criteria and its placement as a category leader in this RiskTech Quadrant®.

Chartis gave SAS a high rating for its data and systems integration capabilities, due to SAS's ability to easily integrate a myriad of third-party and proprietary data, signals and solutions into its transaction monitoring stack, enabled by the deep data orchestration capabilities of the SAS Viya platform. SAS's Financial Crime Decisioning stands out as an AML and financial crime solution tailored for a broad set of financial and non-financial institutions seeking to mitigate risk throughout the customer lifecycle. SAS's use of embedded monitoring of customer lifecycle events, processing both financial and non-financial transactions across different channels and products, makes its transaction monitoring solution notably flexible and adaptable. Enhancement through internal and external data, with real-time enrichment, ensures effective financial crime risk management and false positive reduction.

Vendor Analysis

SAS received a strong rating for its expansive focus on modeling and risk typology capabilities, which enable firms to build a compliant transaction monitoring program with relative ease. Modeling is increasingly critical in enabling enterprise transaction monitoring solutions to tackle the growing complexity that persists in the financial crime ecosystem. SAS offers extensive coverage across the financial crime spectrum, with strong libraries that help address the growing need for typology and channel customization in many high-risk entities.

The critical role of modeling in the transaction monitoring ecosystem points to the fact that tightening regulatory scrutiny, transparency and explainability are rising in prominence. Increasingly, banks and other financial institutions are seeking assistance in explaining models rather than in building them, highlighting the need for a balance between efficiency and expandability within the model risk management (MRM) process. SAS's heritage in model development, maintenance and deployment positions it well in this context, as does the company's commitment and robust approach to model ethics. Additionally, Chartis recognizes that SAS's enhanced user testing for dynamic scenario tuning and optimization, using its ML capability to train rules and models on historical data, is proven to deliver strong results.

SAS's AML transaction monitoring solutions emphasize speed, volume and performance. These solutions are capable of screening transactions in real time, easily integrating with case management systems to ensure prompt action on suspicious activities. Additionally, the platform and solution incorporate real-time watchlist screening, allowing organizations to identify and respond to potential threats quickly. This focus on rapid processing enables financial institutions to manage large volumes of transactions effectively while maintaining robust compliance with regulatory requirements.

Chartis' strong rating for SAS in the workflow automation category reflects the company's cutting-edge AI and ML algorithms. By harnessing the power of large language models (LLMs), SAS creates virtual assistants that streamline such processes as ensuring compliance with FinCEN filing requirements. By automating routine tasks, such as the quality control of narratives, these co-pilots allow users to focus on more complex activities. Additionally, SAS offers AI-driven entity resolution as a 'model as a service', enabling organizations to identify and match entities across diverse data sources. This enhances data integrity and facilitates better decision-making, ultimately making workflows more efficient and effective.

The scores for platform and case management for SAS were also strong. Chartis recognizes the strength, scalability and flexibility of the SAS Viya platform, which was built for performance and has a proven track record of delivering in high-volume, complex environments.

The core technology components of SAS's case management enable end users to review and manage alerts and events, temporarily suppress alerts, reopen closed alerts and initiate cases for further investigation. Multiple alert events are grouped into a single work package, providing users with a holistic view of related information, including previous cases, regulatory filings, customer risk ratings and related fraud activity. End users can connect related customers, alerts, cases or virtually any object within the system. SAS supports this functionality with real-time network and entity generation processes, allowing firms to create network diagrams, resolve real-world entities and reveal hidden relationships using the most current data. Compliance managers can prioritize analyst tasks, track productivity and effectiveness, and adjust surveillance strategies to address new and emerging trends.

SAS's robust solution packaging and deployment capabilities are designed for efficiency and scalability. The company's implementation process and timeline for Tier 1 solutions and beyond are shorter than most, ensuring a swift transition for organizations. The solutions are horizontally scalable, allowing businesses to expand their capabilities as needed. Additionally, SAS provides out-of-the-box ML detection, enabling users to leverage advanced analytics without extensive customization, and making it easier to address complex challenges right from the start.

Vendor Analysis

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

Vendor positioning in context – market potential

SAS's AML transaction monitoring solutions have become established as leaders in transaction monitoring services, and this success contributed significantly to its designation as a category leader in this RiskTech Quadrant®. The company's AML transaction monitoring offerings combine global regulatory compliance with human-led and AI- and ML-driven solutions, a breadth of capabilities that validates the vendor's category leadership.

In particular, the robust ratings for customer success and market penetration reflect the company's expansive, global and diverse client base, which comprises a variety of financial institutions, including banks, credit unions, PSPs and FinTechs.

SAS's strong ratings for growth strategy and financials also bear witness to the continued and increased demand for its services and solutions across North America, Europe, the Middle East and Africa (EMEA), and Asia-Pacific, which has helped to boost client acquisitions. To keep up with this expanding demand, SAS continues to widen its client base across all tiers and areas of focus, alongside its already extensive workforce.

Chartis also found SAS's product and strategic roadmap to be highly competitive and aligned with the direction of the markets it serves.

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

Table 1: Completeness of offering – SAS (AML transaction monitoring solutions, 2024)

Completeness of offering criterion	Coverage
Data and system integrations	High
Focus on modeling and risk typology	High
Focus on speed and volume	High
Platform and case management	High
Workflow automation	High
Solution packaging and deployment	High

Source: Chartis Research

Table 2: Market potential – SAS (AML transaction monitoring solutions, 2024)

Market potential criterion	Coverage
Customer satisfaction	High
Market penetration	High
Growth strategy	High
Business model	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.

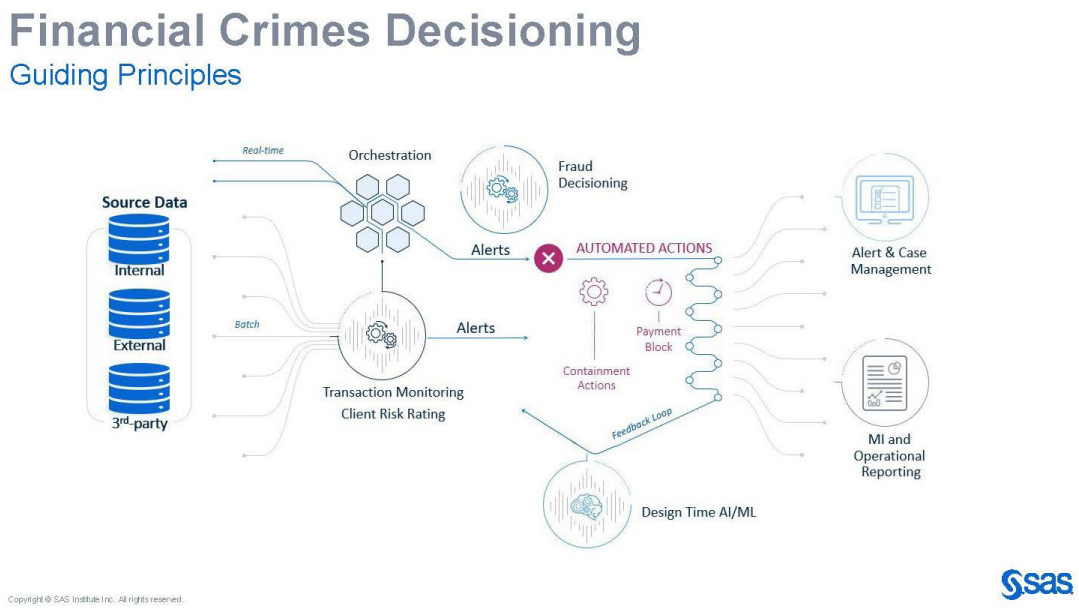
Table 3: SAS Institute Inc. – company information

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 leading 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's fraud and financial crimes clients run the gamut from global systemically important banks (G-SIBs) that rely on SAS solutions for real-time fraud interdiction to small-to-medium institutions that utilize SAS's software to comply with money laundering regulations.
Solution	SAS's fraud and financial crime solutions are built on the SAS® Intelligent Decisioning architecture, which provides a consistent cloud-native technology stack. The SAS® Intelligent Decisioning architecture utilizes orchestration and industry-standard APIs to ingest data into its transaction monitoring environment. The monitoring engine supports Boolean and advanced ML strategies that can be deployed in real time, near-real 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 SAS® Intelligent Decisioning architecture captures outcomes for the reporting and dynamic refresh of signatures.

Source: SAS

SAS's fraud and financial crime solutions are built on a common technology architecture that can be deployed to address both fraud risks and money laundering/terrorism financing risks. Figure 2 illustrates the primary functional components.

Figure 2: SAS financial crime decisioning



Source: SAS

SAS® Anti-Money Laundering software includes intellectual property for mapping transaction, account and entity dimensions in support of both transactional and non-transactional AML monitoring strategies. Increasingly, clients are using data orchestration to enrich monitoring or investigative processes with third-party data (e.g., risk ratings of virtual asset service providers). As part of the SAS® Viya® 4 cloud-native architecture, the solution is designed to optimize and govern the use of open-source programming languages (R, Python, Lua, etc.) for clients that wish to augment their existing processes with AI and ML.

SAS® Anti-Money Laundering software features 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 as well as advanced alert scoring. Many clients use advanced scoring logic to automate the triage of alerts to investigation. SAS's new case management tool is highly configurable to support a wide range of financial crime investigations. The tool supports elastic search and provides dynamic link analysis as a standard OOTB feature.

Beginning with the SAS® Viya® 4 release, SAS® Customer Due Diligence is included with SAS® Anti-Money Laundering software, to give firms 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.

Once events have triggered a review or investigation, work items persist in SAS's alert and case management tool. Screens have been configured for specific types of activities, including 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.

Vendor Analysis

Many SAS clients leverage the 'design time' financial crime analytics capabilities found in SAS's award-winning ML tools. SAS supports the entire AI life cycle from data acquisition to champion-challenger design and testing of strategies to deployment. SAS's natural language processing (NLP) methods have been effective in detecting trade-based money laundering risks that are hidden in text in unstructured data (letters of credit, goods descriptions, etc.)

Vendor leading practices

SAS is a leader in AI/ML, with more than 20 years' experience in deploying fraud and financial crime solutions to global clients. It has a tremendous amount of institutional knowledge that varies from fraud disciplines to compliance disciplines. SAS's Risk, Fraud and Compliance Solutions team understands both the business requirements for risk management and the steps required to satisfy model governance concerns that are top of mind with the deployment of AI.

SAS's expertise in analytics allows the company to help clients adopt more innovative strategies for managing AML compliance risks. SAS's subject matter experts support clients through:

- Periodic health checks to assess the efficacy of monitoring programs.
- Proven techniques for progressing clients on their 'NextGen' journey to adopt anomaly detection, behavioral segmentation, process automation and ML-based detection strategies.
- Recommended strategies for tagging investigation outcomes to inform tuning/optimization.
- Advanced ML methods for entity resolution.
- ML models for client risk rating.
- API strategies for enriching and automating the use of third-party data to reduce manual processes.

SAS has formed a new group within its R&D division that is focused on developing AI/ML models as OOTB offerings. This year, the company has released the following models that support fraud and financial crime:

- SAS® AI-Driven Entity Resolution.
    - Streamlines decision-making and boosts operational efficiency by accurately identifying and consolidating entities across various datasets. This model offers robust data preparation, flexible fuzzy matching and scoring to eliminate duplicates and inconsistencies, ensuring a single, accurate view of each entity. By increasing accuracy and reducing errors, this model enhances data quality, saves time and cuts costs.
- SAS® Document Analysis.
    - Transforms scanned document images into structured data for reporting and analytics with an intelligent document processing (IDP) pipeline. SAS® Document Analysis cloud-based optical character recognition (OCR) includes models and utilities that streamline text extraction, making it accessible across a multitude of users. It simplifies digital transformation for such compliance use cases as TBML, by converting unstructured data into usable formats, optimizing batch processing and supporting robotic process automation.

As organizations explore GenAI, SAS prioritizes the identification of high-ROI, ethically applied use cases. The company aims to enable secure adoption, fostering accelerated productivity, trusted results and faster innovation across diverse industries and regulatory landscapes.

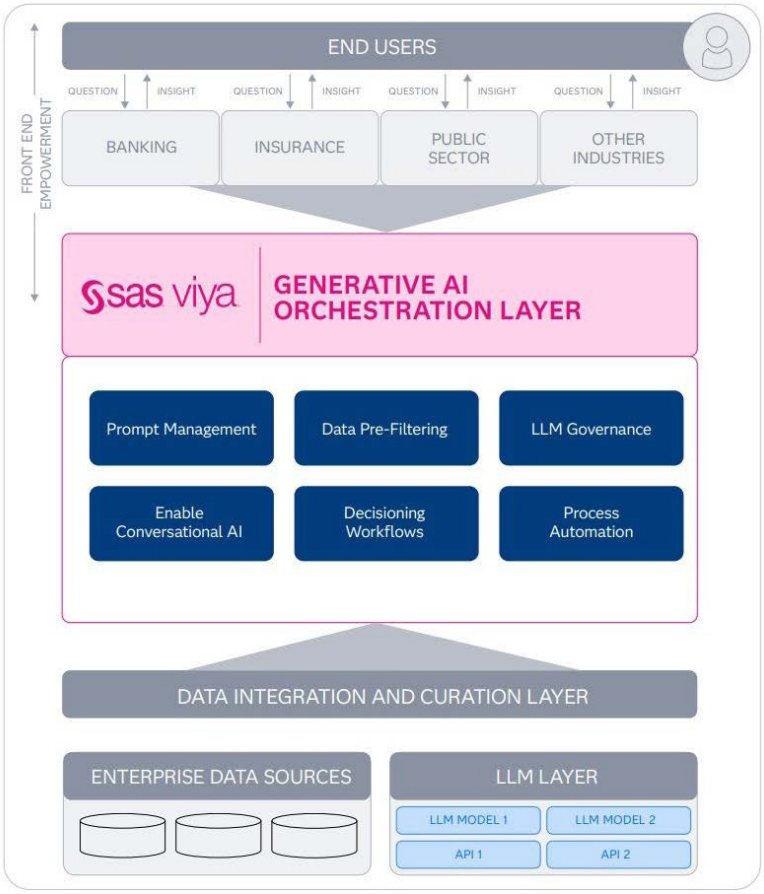
SAS provides software and services that include:

- GenAI with SAS® Viya® – integrates external GenAI models, orchestrating large language models (LLMs) for end-to-end enterprise use cases.
- Viya® Copilot – a personal assistant to accelerate development, business and industry tasks for increased productivity. It offers diverse tools for such tasks as data cleaning, exploration, model execution and dashboard generation.
- SAS® Data Maker – addresses limited real data challenges by generating high-quality synthetic tabular data that is statistically representative of the original training data, without compromising sensitive information.

The SAS difference

- **Accelerated innovation**. SAS transforms LLMs into actionable insights by seamlessly integrating GenAI models into decisioning workflows, AI/ML applications and existing business processes.
- **Data protection**. SAS upholds user privacy and security with robust data protection measures, including data minimization, anonymization and encryption, ensuring that sensitive information remains safeguarded.
- **Trustworthy results**. SAS applies natural processing techniques to pre-process data, ensuring that only high-quality data is fed to LLMs, minimizing computational waste, reducing costs and producing reliable outcomes.

Figure 3: SAS Viya®



Source: SAS

- **Enhanced governance**. SAS's built-in workflows validate the entire life cycle of LLMs, from regulatory compliance to model risk management. Additionally, SAS offers responsible ideation, experimentation and operationalization support.
- **Precise decisioning**. Quantitative decisioning capabilities, critical for successful GenAI reasoning, are built into the Viya® platform (see Figure 3).

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 appreciate the rationale for our analysis. The specific criteria used for AML Transaction Monitoring Solutions, 2024 are shown in Table 4.

[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.*

Table 4: Evaluation criteria for Chartis' AML transaction monitoring solutions, 2024 report

Completeness of offering	Market potential
• Data and system integrations	• Customer satisfaction
• Focus on modeling and risk typology	• Market penetration
• Focus on speed and volume	• Growth strategy
• Platform and case management	• Business model
• Workflow automation	• Financials
• Solution packaging and deployment	

Source: Chartis Research

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 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. Rather, our ranking methodology highlights 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.

Vendor Analysis

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