Market Quadrants

Chartis

AML Transaction Monitoring Solutions, 2025

Quadrant Update



06 NOV 2025

Vendor Landscape Report

Authors
Sean O'Malley and Jason Wright

For details of Chartis' research methodology, ***click here****.*

Jump to: **Market landscape** | **Vendor landscape** | **Quadrant dynamics** | **Chartis RiskTech Quadrant® and tables** | **What to watch**

Executive summary

This report provides Chartis' latest view of the vendor landscape for anti-money laundering (AML) transaction monitoring solutions, updating and expanding on our previous research in ***AML Transaction Monitoring Solutions, 2024: Quadrant Update*** and ***AML Transaction Monitoring Solutions, 2024: Market Update***, both published in October 2024.

The AML transaction monitoring market in 2025 is defined by diversification, technological acceleration and a sharp increase in regulatory expectations. As financial crime evolves and institutions face mounting pressure to modernize their compliance operations, vendors are now being assessed not only on their ability to detect suspicious activity, but also on the adaptability, scalability and intelligence of their broader solutions.

Reflecting the increasingly interconnected nature of financial crime and compliance challenges, this report provides a unified view of the vendor landscape across traditional transaction monitoring, integrated risk intelligence and case management capabilities – areas that were previously assessed separately. It also offers a consolidated view of the market landscape and

positions key providers in our AML transaction monitoring solutions quadrant.

Several themes have emerged across the market:

- **Strategic segmentation**. Vendors are pursuing distinct approaches, from broad enterprise compliance suites to specialized point solutions tailored for FinTechs or regional institutions. Some are building horizontal platforms that unify AML, fraud and conduct risk, while others are focusing on deep functionality in transaction typologies or high-risk geographies.
- **AI and automation**. Reducing false positives remains a key driver, with explainable artificial intelligence (AI), behavioral analytics and automation at the core of next-generation monitoring. Model transparency and governance are no longer optional; they are baseline expectations in regulated environments.
- **Operational integration**. Vendors are embedding monitoring tools into broader compliance workflows, case management systems and investigative platforms. Modular deployment and open integration capabilities have become essential, especially for institutions assembling best-of-breed compliance stacks.
- **Regional intelligence**. Many providers are deepening their support for localized regulations and typology libraries, reflecting growing demand for jurisdiction-specific agility, particularly in the Middle East, Southeast Asia and emerging markets.

As highlighted in the quadrant and vendor capabilities section, this year's RiskTech Quadrant® for AML transaction monitoring solutions shows greater segmentation than previous ones, with clearer distinctions in how vendors align with different customer profiles and solution strategies. From global

platforms to agile innovators, all vendors occupy important positions within the ecosystem, reflecting the diversity of customer needs, risk appetites and operating models.

Chartis uses the RiskTech Quadrant® to explain the structure of a market. The RiskTech Quadrant® employs a comprehensive methodology of in-depth independent research and a clear scoring system to explain which technology solutions meet an organization's needs. The RiskTech Quadrant® does not simply describe one technology solution as the best; rather, it has a sophisticated ranking methodology to explain which solutions best fit buyers' implementation strategies.

This report covers the following providers of AML transaction monitoring solutions:[1] Abrigo, ACTICO, Acuminor, AlertSpeed, AP Solutions IO, Azentio, BPC, Clari5, Cleareye.ai, ComplyAdvantage, Complytek, Data Gear, DataVisor, Discai, Eastnets, Feedzai, Fenergo, FIS, Flagright, Flaminem, GBG, Genpact riskCanvas, Hawk, IMTF, LexisNexis Risk Solutions, Linkurious, Lucinity, Manipal Group, Mozn, MyComplianceOffice, Napier AI, Nasdaq Verafin, NetGuardians (Vyntra), NICE Actimize, Oracle, Oscilar, Prometeia, PwC, Quantexa, Salv, SAS, SGR Compliance, Silent Eight, Solytics Partners, Sumsub, SymphonyAI, ThetaRay, Tookitaki, Transvision Solutions, Trapets, Unit21, Vneuron and Wibmo.

Back to top

Context: market landscape

AML transaction monitoring continues to evolve under the weight of changing financial crime patterns, regulatory scrutiny and technology innovation. Financial institutions face a dual mandate: maintain compliance while improving operational efficiency and customer experience.

Legacy systems still dominate much of the market, but their limitations, such as high false positive rates and a lack of

adaptability, are pushing investment toward modern, data-driven solutions. Cloud-native platforms, graph analytics and behavioral detection models are gaining traction. At the same time, regional fragmentation in regulations and uneven technological maturity across institutions have created a very heterogeneous market. This diversity is prompting both vendors and financial institutions to adopt modular, flexible approaches to transaction monitoring.

As regulatory expectations rise and criminals become more agile, institutions that fail to modernize their systems risk falling behind – both in their compliance and in their effectiveness in combatting fraud.

Market updates since our previous report

- **An exponential increase in regulatory scrutiny, enforcement and fines**. In 2025, global regulatory bodies have sharply escalated their enforcement actions tied to deficiencies in AML transaction monitoring. In the UK, **the Financial Conduct Authority (FCA) fined Monzo Bank £21.1 million** (approximately US$28.2 million) for "inadequate anti-financial crime systems and controls", including failures in customer onboarding, risk assessment and transaction monitoring that did not scale alongside the bank's rapid growth. **The FCA also fined Barclays £42 million** (US$56.2 million) for separate instances of financial crime control failings. Barclays failed to gather sufficient information before opening certain accounts and failed to assess risk properly. Meanwhile, Canada's Financial Transactions and Reports Analysis Centre (FINTRAC) has imposed several penalties, fining **Crystal Currency Exchange about CAD348,000** (US$250,000) for multiple AML regime violations, including a failure to report suspicious transactions, and **Cambrian Credit Union CAD116,160** (US$83,000) for reporting and risk assessment lapses. These actions highlight a regulatory climate in which

large financial institutions and smaller reporting entities are being held to strict standards. They also corroborate aggregate industry reports that suggest a steep upward trajectory in AML-related penalties, and underscore that weak transaction monitoring is increasingly seen as a regulatory risk, not just a compliance burden.

- **Advancements in AML technologies and strategies**. In 2025, regulatory and structural shifts are accelerating the adoption of advanced technologies in AML, signaling a new phase of compliance modernization. Global regulators are not only tightening their oversight, but also expanding the scope of AML obligations, notably through moves like the U.S. Final Investment Adviser Rule and evolving legislation regarding digital assets and stablecoins, which are bringing new sectors and products under AML scrutiny. In parallel, advances in AML technology, including the rise of AI, graph analytics and explainable machine learning (ML), are transforming how firms detect, investigate and report suspicious activity. Tools leveraging behavioral modeling, entity resolution and real-time monitoring are increasingly being adopted to manage growing transaction volumes and complexity. Moreover, there is a push for models that are not just performant but also interpretable and auditable, as regulators emphasize the need for transparent decision-making in automated systems. This convergence of regulatory expectations and technological capabilities is driving a structural shift in AML – from compliance as a static function to a dynamic, data-driven risk management discipline.
- **Dynamics, risks and pressures in the marketplace**. A growing challenge in the AML transaction monitoring space is the compounding impact of false positive fatigue and the high cost of legacy system migration. As transaction monitoring systems become more complex and thresholds are adjusted downward in response to regulatory pressure, financial institutions are experiencing a surge in low-value alerts,

overwhelming compliance teams and creating significant backlogs. This alert overload not only strains resources but also diverts attention from genuinely suspicious activity, undermining the effectiveness of AML programs. At the same time, many large institutions remain burdened by outdated, rules-based systems that are deeply embedded in legacy infrastructure. The cost and complexity of upgrading to modern, AI-enabled platforms are substantial, often requiring parallel operations, data migrations and regulatory revalidation. Chartis recommends that firms should have a well-managed transition strategy. Otherwise, they risk becoming stuck in a costly 'mid-modernization' phase, where outdated systems persist alongside underutilized new solutions, leading to operational inefficiencies and continued regulatory exposure.

Back to top

Vendor landscape: overview

The vendor landscape is evolving rapidly, driven by heightened regulatory scrutiny, advances in AI and the increasing complexity of financial crime schemes. Vendors in the AML transaction monitoring space are expanding their focus beyond traditional rules-based detection systems to incorporate sophisticated ML models, behavioral analytics and real-time monitoring capabilities. This shift reflects a broader industry trend toward more adaptive, predictive and context-aware solutions that can effectively identify emerging threats and reduce false positives.

In addition to enhanced detection technologies, many vendors are integrating comprehensive case management and workflow automation tools, enabling seamless collaboration between compliance teams and improving operational efficiency. Cloud-based deployments and application

programming interface (API)-driven architectures are becoming increasingly prevalent, allowing for faster implementation, scalability and integration with broader risk and compliance ecosystems.

These advances significantly influence end-customers' decision-making processes. Organizations now prioritize vendors that offer not only robust detection accuracy but also transparency, explainability of alerts and ease of integration with existing systems. The growing emphasis on user experience and automation helps reduce manual investigation burdens, allowing compliance officers to focus on high-risk cases with greater confidence. Furthermore, as regulatory expectations evolve, customers are seeking vendors that provide flexibility and ongoing adaptability to ensure continued compliance in a dynamic risk environment.

Overall, the current vendor landscape highlights a move toward intelligent, agile and customer-centric AML transaction monitoring solutions, reshaping how financial institutions approach their AML efforts and risk mitigation.

Back to top

Quadrant dynamics: which types of firms are winning?

In its quadrant reports, Chartis assigns each vendor a numerical 'completeness of offering' set of scores (previous reports used an asterisk key). We believe this provides a clearer assessment of the breadth and scope of each firm's solution capabilities within the overall vendor landscape.

Chartis' RiskTech Quadrants® enable an understanding of the relative position of solutions and providers in a particular market segment. We present a comparison that aligns market potential with completeness of offering. Distinction among the

four areas of the quadrant rests on the scope of the offering/solution and the vendor's business strategy – specifically, its effectiveness with its target buyers.

- **Category leaders** achieve this distinction because they exhibit strength across the broadest set of capabilities in the segment, showing clear execution of core strategy and innovation.
- **Best-of-breed** solutions provide class-leading capabilities in specific areas or functions and are often deployed to address a particular need or use case.
- **Point solutions** may not have as many capabilities as 'category leaders' or 'best-of-breed' solutions, but their functionality may be a perfect fit for institutions seeking domain-specific capabilities. And given their deep focus on a relatively narrow area, point solution providers are often more able and willing to innovate quickly compared to vendors that offer a broader technology scope.
- **Enterprise solutions** are established platforms with demonstrated integration and scalability.

Vendor archetypes in 2025

- **Enterprise suite leaders**. These vendors offer comprehensive financial crime and compliance platforms that go far beyond transaction monitoring – often encompassing case management, Know Your Customer (KYC)/customer due diligence (CDD), sanctions, fraud and even environmental, social and governance (ESG) or operational risk. They compete on breadth, proven scalability and deep regulator-facing credibility and trust, often becoming long-term strategic partners to Tier 1 banks and large financial institutions.
- **AI-native and real-time innovators**. These providers are

disrupting traditional rules-based monitoring with explainable AI, real-time behavioral analytics, continuous learning systems and faster time to value. Focused on false positive reduction, adaptive modeling and automation, they offer flexible, cloud-native tools that appeal to digital-first banks and FinTechs.

- **Risk intelligence and data-enrichment providers**. These players enhance transaction monitoring systems by providing contextual risk intelligence, often involving adverse media, ultimate beneficial ownership (UBO) data, network analytics and typology-based risk mapping. They often integrate with core systems to improve alert triage, risk assessments and the quality of suspicious activity reports (SARs) and currency transaction reports (CTRs).
- **Regional and segment specialists**. These vendors deliver specific, tailored AML solutions optimized for regional- or segment-based regulatory frameworks (e.g., Islamic finance, payment processors, government banks). Their strengths lie in deep regulatory localization and cultural/regional nuance, local language support, regional datasets and pre-built, domain-specific compliance templates.
- **Infrastructure, advisory and embedded enablers**. These firms either act as transformation enablers (consulting-led, process-centric vendors) or offer embedded, AML-as-a-service capabilities suitable for FinTechs and smaller institutions. Some offer identity verification, risk controls or managed services that complement core AML systems.

Back to top

Chartis RiskTech Quadrant® and vendor capabilities for AML transaction monitoring solutions, 2025

The AML transaction monitoring market remains specialized yet intensely competitive, with rapidly evolving differentiation factors. Vendors that historically competed primarily on detection accuracy and compliance with regional regulations are now being evaluated on their ability to provide comprehensive, adaptable solutions that address complex, multijurisdictional risks and emerging financial crime typologies.

In 2025, the focus has shifted toward vendors' capacity to deliver scalable, AI-driven monitoring that not only detects suspicious activity but also supports operational resilience under evolving regulatory frameworks. Increasingly, clients demand platforms that can integrate cross-asset transaction data, incorporate risk intelligence and automate workflows to reduce false positives and investigative burdens.

We observed several defining trends that are shaping our quadrant's structure:

- A growing emphasis on explainable AI and model governance to satisfy regulatory scrutiny.
- The continued importance of geographic and sector specialization, reflecting the diversity of global regulatory expectations.
- The rise of cloud-native, API-driven architectures that enable faster deployment and integration with broader compliance ecosystems.
- Customer expectations for platforms that support agile rule configuration, seamless case management and real-time alerts.

Compared to last year's **AML transaction monitoring solutions quadrant report**, this year's analysis features significantly more segmentation and a clearer separation of vendors, reflecting the increasing diversity and specialization within the AML transaction monitoring market. Our goal was to represent the vendor landscape more accurately by highlighting each provider's unique strengths relative to their target markets and core technology capabilities. This approach allows for a nuanced view that distinguishes vendors not only by their overall market impact but also by their strategic focus, whether on innovation, regional expertise, operational efficiency or integrated risk intelligence. This offers buyers a clearer perspective on which solutions best align with their specific AML priorities.

Figure 1 illustrates Chartis' view of the vendor landscape for AML transaction monitoring solutions.[2] Table 1 lists the completeness of offering criteria we used to assess the vendors. Table 2 lists the vendor capabilities in the AML transaction monitoring category.

Figure 1: RiskTech Quadrant® for AML transaction monitoring solutions, 2025



Source: Chartis Research

Table 1: Assessment criteria for vendors of AML transaction monitoring solutions, 2025

Assessment criterion	What good looks like
Data and system integrations	A comprehensive AML transaction monitoring solution must offer seamless integration with a wide variety of internal and external systems, including core banking platforms, KYC/CDD tools, watchlists and third-party risk data providers. It should support both batch and real-time data ingestion through APIs, streaming services and secure file transfers, enabling scalable, low-latency pipelines that maintain data quality across diverse sources. Deep interoperability with case management, workflow and customer relationship management (CRM) systems is essential to provide a unified view of risk and streamline operational processes.
Risk typology modeling	The platform should provide an extensive and adaptable library of risk typologies aligned with such global regulatory frameworks as the Financial Action Task Force (FATF), supporting the identification of both standard and emerging money laundering methods. It needs to allow risk teams to easily customize and create new typologies using intuitive interfaces, without heavy reliance on IT departments. The flexibility to update typologies quickly in response to evolving threats and regulatory expectations, along with detailed audit trails, ensures transparency and governance for compliance teams.
Analytical modeling	Effective AML monitoring solutions leverage advanced analytical techniques, including heuristic rules and ML algorithms, to detect suspicious activity. They should offer transparent, interpretable models that support explainability for regulatory scrutiny and enable real-time scoring with automated retraining on fresh data. Such sophisticated capabilities as behavioral analytics, peer group comparisons and scenario stress testing enhance detection power and reduce false positives, ensuring a balanced approach to risk identification.
Model quality and validation	Robust model quality assurance is critical, with built-in validation frameworks that align with industry standards and regulatory guidance. The solution should provide quantitative performance metrics, including accuracy, recall and false positive rates, and support back-testing and drift monitoring to maintain ongoing model effectiveness. Features like version control, independent validation tooling and comprehensive documentation enable organizations to defend their models confidently during regulatory reviews.
Focus on speed, volume and performance	A high-performing AML system must process millions of transactions per day with minimal latency, ensuring that suspicious activity is detected in near-real time. Cloud-native, horizontally scalable architectures with redundancy and failover guarantee resilience and uninterrupted service even under peak loads. Clear performance metrics on throughput and latency, demonstrated success in rigorous external benchmarks and a careful balance between processing speed and detection accuracy distinguish top-tier platforms that can handle large-scale, complex environments.
Workflow automation	Automation is key to efficient AML operations, and best-in-class solutions provide end-to-end workflow orchestration for alert triage, case management and reporting. Intelligent alert prioritization, suppression rules and dynamic routing streamline investigator workloads, while embedded tools facilitate evidence collection, annotation and SAR drafting with compliance-ready templates. Integration with external governance, risk and compliance (GRC) platforms or law enforcement portals via APIs further enhances operational efficiency and oversight.
Solution packaging and deployment	The ideal AML transaction monitoring vendor offers flexible, modular packaging that can be deployed rapidly either on-premises, in hybrid configurations or as fully cloud-native solutions across major cloud providers. It supports continuous integration and delivery pipelines to enable quick updates, version control and easy rollback. With transparent documentation and configuration options accessible to non-technical users, deployments can be completed in weeks, not months, accelerating time-to-value while ensuring ongoing adaptability and vendor support.

Source: Chartis Research

Table 2: Vendor capabilities for AML transaction monitoring solutions, 2025

Vendor	Data and system integrations	Risk typology modeling	Analytical modeling	Model quality and validation	Focus on speed, volume and performance	Workflow automation	Solution packaging and deployment
Abrigo	3.9	4.5	4.2	2.5	3.3	3.4	3.2
ACTICO	3.4	4.5	4.5	4.5	4.1	3.3	3.2
Acuminor	2.2	4.5	2.1	3.2	2.3	2.3	2.5
AlertSpeed	4.2	4.2	4.5	4.2	2.3	2.9	3.3
AP Solutions IO	2.3	4.5	1.7	2.3	1.7	2.7	3.5
Azentio	3.3	4.5	4.1	3.9	2.8	3.3	3.3
BPC	3.8	4.5	3.6	2.7	4.0	3.1	3.2
Clari5	4.2	4.5	3.7	2.7	4.2	2.7	3.3
Cleareye.ai	2.9	1.7	3.7	2.7	3.3	3.2	3.7
ComplyAdvantage	3.1	3.4	4.2	3.1	3.2	2.8	3.6
Complytek	1.7	1.7	3.7	3.8	3.5	3.1	3.2
Data Gear	4.5	4.5	4.1	3.6	3.6	2.7	2.3
DataVisor	2.9	4.5	4.1	3.8	3.8	3.7	3.3
Discai	2.7	3.9	3.4	4.1	4.1	3.2	3.4
Eastnets	4.3	4.5	3.9	4.1	3.7	3.6	3.7
Feedzai	4.1	3.3	4.2	3.7	4.1	3.4	3.7
Fenergo	3.2	4.5	4.0	3.7	3.7	4.1	3.7
FIS	3.2	3.1	3.7	3.8	1.7	3.6	3.8
Flagright	4.3	4.5	4.0	3.8	4.7	4.3	2.9
Flaminem	2.7	3.6	3.7	3.3	2.1	3.2	3.2
GBG	3.7	4.5	3.9	3.4	3.6	3.2	3.3
Genpact riskCanvas	2.8	4.5	3.7	3.6	4.2	3.4	2.8
Hawk	3.0	4.1	3.8	3.3	4.7	4.1	3.6
IMTF	4.5	4.5	4.2	3.8	4.2	4.2	3.6
LexisNexis Risk Solutions	4.5	4.5	3.3	3.3	3.7	3.3	3.6
Linkurious	4.5	4.5	3.7	1.7	3.5	2.4	2.7
Lucinity	4.4	4.5	3.3	3.5	4.3	3.7	2.8
Manipal Group	4.2	4.2	4.5	3.8	3.4	3.6	3.4
Mozn	4.2	4.1	4.0	3.8	4.3	4.2	3.5
MyComplianceOffice	3.3	4.5	3.3	3.3	3.8	3.8	3.3
Napier AI	3.5	4.1	4.5	3.5	2.3	3.7	3.2
Nasdaq Verafin	3.8	4.5	4.2	3.3	4.6	4.2	3.7
NetGuardians (Vyntra)	2.7	3.8	3.8	3.2	3.7	2.7	3.2
NICE Actimize	3.6	4.1	4.2	3.8	4.4	4.6	3.7
Oracle	4.2	4.5	4.1	4.3	4.5	4.1	4.1
Oscilar	4.4	4.5	4.2	3.7	4.2	4.3	3.7
Prometeia	2.4	4.5	3.3	3.8	1.7	3.4	3.3
PwC	4.5	4.5	4.2	4.4	2.8	3.6	3.3
Quantexa	3.9	3.8	3.7	3.8	4.0	3.8	3.5

Key: 1.0–2.0: Partial coverage/Component capability; 2.1–3.0: Meeting industry standards; 3.1–4.0: Advanced capabilities; 4.1–5.0: Best-in-class capabilities

Continued on page 16

Table 2: Vendor capabilities for AML transaction monitoring solutions, 2025

Vendor	Data and system integrations	Risk typology modeling	Analytical modeling	Model quality and validation	Focus on speed, volume and performance	Workflow automation	Solution packaging and deployment
Salv	2.7	4.5	3.3	3.2	3.6	2.8	3.3
SAS	3.0	4.5	3.9	3.9	4.4	4.5	3.2
SGR Compliance	3.6	3.7	4.1	2.1	2.1	3.7	2.9
Silent Eight	3.2	3.7	4.3	3.7	3.7	3.8	3.8
Solytics Partners	4.5	4.5	4.1	3.9	4.3	3.4	3.4
Sumsub	4.1	4.5	4.3	2.7	3.6	3.7	3.4
SymphonyAI	4.2	3.8	4.2	3.9	4.4	4.1	3.8
ThetaRay	3.9	4.5	3.7	4.3	4.5	4.5	3.3
Tookitaki	4.4	4.5	4.3	3.7	3.9	4.1	3.5
Transvision Solutions	2.9	4.5	3.3	3.7	3.8	3.9	3.2
Trapets	3.3	3.6	3.5	2.7	3.7	2.7	2.9
Unit21	2.9	4.5	3.7	3.6	4.5	3.8	3.1
Vneuron	3.2	4.5	3.7	4.2	4.3	3.2	2.7
Wibmo	2.2	4.5	2.1	2.7	3.3	2.4	2.3

Key: 1.0–2.0: Partial coverage/Component capability; 2.1–3.0: Meeting industry standards; 3.1–4.0: Advanced capabilities; 4.1–5.0: Best-in-class capabilities

Source: Chartis Research

Winning firms

Each quadrant reflects a valuable and viable approach, aligned to different organizational priorities and compliance strategies. There is no 'bad' quadrant, only distinct strengths suited to varied customer needs.

Category leaders represent vendors with a strong market presence and comprehensive technology offerings, often delivering end-to-end AML transaction monitoring solutions trusted by large, complex institutions. Their breadth and depth make them ideal for organizations seeking a fully integrated platform.

Enterprise solution vendors provide robust, mature platforms that serve a wide range of customer needs with strong regulatory alignment and operational reliability. They are well-suited to enterprises that require proven, adaptable solutions that balance functionality and integration across multiple compliance areas.

Best-of-breed vendors focus on innovation and specialized capabilities, often leveraging cutting-edge AI, advanced analytics or domain expertise. These solutions excel in specific AML use cases or market segments, offering agility and precision for organizations looking to complement or enhance their existing compliance infrastructure.

Point solutions address targeted needs within the AML transaction monitoring ecosystem, such as regional compliance, specific asset classes or niche workflows. These vendors provide focused, efficient tools that fit well in institutions seeking tailored functionality or incremental improvements without having to overhaul entire systems.

Back to top

What to watch

Chartis expects several themes to develop over the next 12 months:

- **Convergence of AML, fraud and risk**. Institutions are increasingly seeking unified platforms that can address multiple financial crime risks. Vendors that can design modular, interoperable solutions, allowing AML to integrate with fraud detection, sanctions screening and conduct surveillance, will gain a strategic advantage.
- **Explainability, not just accuracy**. As regulators demand transparency in AI models, vendors must prioritize explainability, model governance and auditability. Black-box AI is becoming a liability. Vendors should invest in interpretable ML, robust validation frameworks and tools that support defensible decision-making.
- **Domain-aware AI and typology libraries**. Generic anomaly detection is no longer enough. Vendors will need to embed domain expertise directly into models through typology-driven analytics, threat libraries and behavior-specific scenarios. Solutions that can adapt to evolving typologies without manual reconfiguration will stand out.
- **Embedded compliance and FinTech enablement**. As embedded finance grows, there is increasing demand for light, API-first AML modules designed for digital-native institutions. Vendors should consider strategies to 'scale down' their offerings without sacrificing control or compliance integrity.
- **A stronger regional focus and regulatory agility**. New regulations in such regions as the Gulf, Southeast Asia and Africa are creating space for regionally fluent providers. Global vendors will need to balance scale with localization, while regional specialists must demonstrate an ability to keep pace with shifting standards.

Back to top

Notes

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

2. Note that the following vendors were contacted during the briefing stage, but either did not respond or declined to participate: Dixtior and Syngo (did not respond), Refine Intelligence and WorkFusion (declined to participate).

Back to top

Copyright Infopro Digital Limited. All rights reserved.

As outlined in our terms and conditions, **https://www.infopro-digital.com/terms-and-conditions/subscriptions/** (point 2.4), printing is limited to a single copy.

If you would like to purchase additional rights please email **info@chartis-research.com**