Vendor Analysis

Vendor Analysis: Pega

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

Chartis

Independent. Insightful. Actionable.

About Chartis

Chartis Research is the leading provider of research and analysis on the global market for risk technology. It is part of Infopro Digital, which owns market-leading brands such as Risk and Waters Technology. Chartis's goal is to support enterprises as they drive business performance through improved risk management, corporate governance and compliance and to help clients make informed technology and business decisions by providing in-depth analysis and actionable advice on virtually all aspects of risk technology. Areas of expertise include:

- Credit risk
- Operational risk and governance, risk and compliance (GRC)
- Market risk
- Asset and liability management (ALM) and liquidity risk
- Energy and commodity trading risk
- Financial crime including trader surveillance, anti-fraud and anti-money laundering
- Cyber risk management
- Insurance risk
- Regulatory requirements including Basel 2 and 3, Dodd-Frank, MiFID II and Solvency II

Chartis is solely focused on risk and compliance technology, which gives it a significant advantage over generic market analysts.

The firm has brought together a leading team of analysts and advisors from the risk management and financial services industries. This team has hands-on experience of implementing and developing risk management systems and programs for Fortune 500 companies and leading consulting houses.

Visit **www.chartis-research.com** for more information.

Join our global online community at **www.risktech-forum.com**.

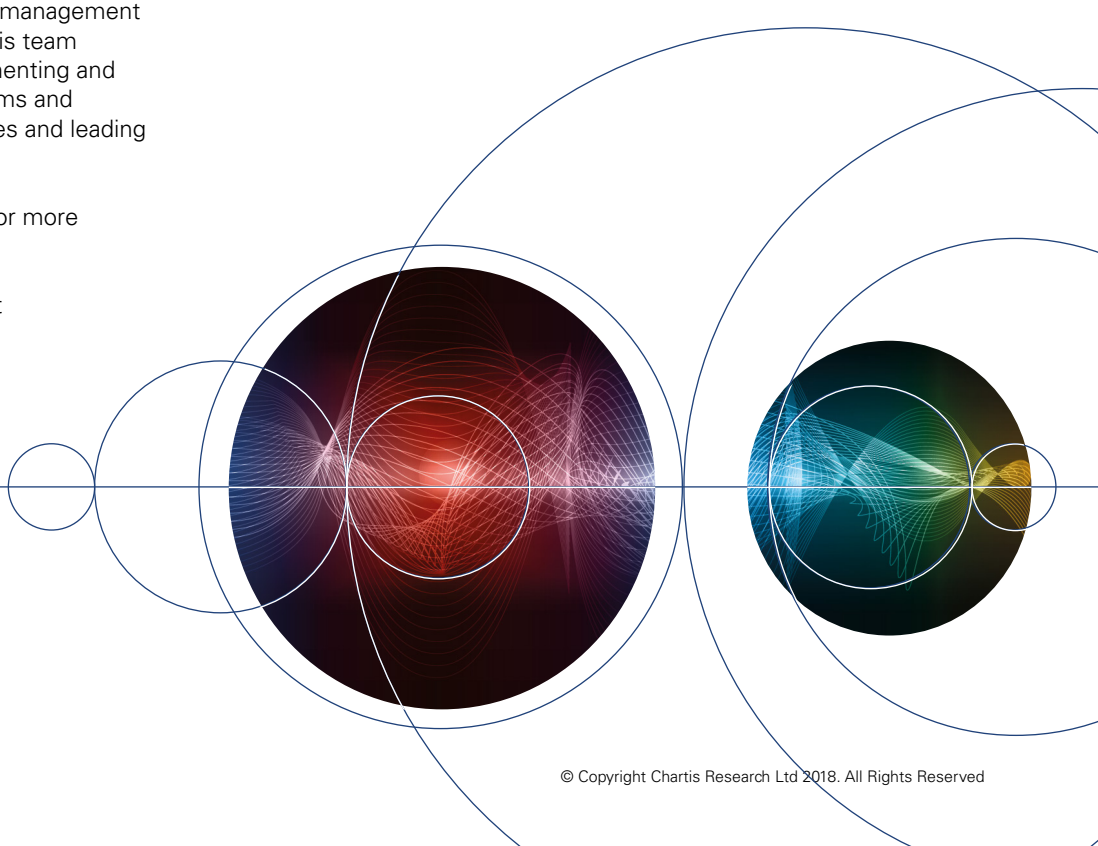


Table of contents

List of figures and tables

1. Report context

This Vendor Analysis is based on the Chartis quadrant report *Financial Crime Risk Management Systems: Know Your Customer; Market Update 2018* (published in August 2018). This section summarizes the key theses in that report; subsequent sections take a detailed look at Pega's quadrant positioning and scoring, and Chartis' underlying opinion and analysis.

Key thesis

The phrase 'Know Your Customer' (KYC) may sound like a business school management course mantra. In financial services, however, KYC is an important, formalized process, one that has become more complex and workload-intensive in recent years. At its core, KYC is concerned with determining the accurate identity of a customer – a person or a company – and then assessing the risk to a Financial Institution (FI) of conducting business with that entity.

For FIs, the KYC process is now increasingly complicated. To verify a potential customer's identity and examine their risk, KYC analysts must consult a vast, and growing, array of data sources.

Within *retail KYC* – which deals with individuals – these information sources include:

- Lists of government-sanctioned entities.
- Lists of Politically Exposed Persons (PEPs).
- Registries of company ownerships and directorships.

Within *wholesale KYC* – which deals with firms – the information sources include:

- Lists of government-sanctioned entities.
- Lists of state-owned enterprises.
- Company ownership and financial data.
- News coverage of particular firms and entities.

Complicating things further, the exact information that an FI must consult and verify varies greatly across different regulatory jurisdictions. This means that a single, central KYC function may not be enough to deal with different rules around the globe.

With massive datasets to sift through – each with its particular regional quirks and requirements – the numbers of KYC staff FIs employ have risen rapidly. FIs are also becoming more concerned with the risk to their reputation of being accused of helping an entity evade sanctions, even indirectly. This has sharpened their focus on Know Your Third Party (KY3P) and Know Your Customer's Customer (KYCC) – further pushing up the size of their KYC departments.

For years, technology solutions for KYC promised unrealistic results, but FIs are now re-examining how vendors can help them cut costs and improve their operational efficiency. Vendors are responding primarily with technical solutions augmented by large service components. In fact, we estimate that services now comprise a larger proportion of vendor revenue from KYC implementations, although technical advances have continued to provide a strong backbone for vendors' KYC solutions. With this technology/services blend, vendors have focused less on replacing staff outright than on assisting FIs' KYC employees by cutting down on menial tasks.

Vendor innovation is being driven by four key technologies and service models:

- **Workflow automation**. Systems powered by Robotic Process Automation (RPA) and Artificial Intelligence (AI) that reduce much of the repetitive work that KYC analysts engage in (such as document and data retrieval).
- **Profile enrichment**. Third-party data repositories that contain lists of sanctioned entities or details of company ownership structures. These reduce the time that employees spend searching disparate sources for the information they need.
- **Consortia and data sharing**. An organized network of FIs, often anchored around a vendor that provides the requisite infrastructure. These FIs share information, so that customers onboarded at one FI can be assessed more rapidly for another institution.
- **Entity resolution and graph analytics**. Systems to identify customers and prevent duplicate accounts or impersonation. Graph analytics aims to do this using networks to determine identities more precisely and confidently.

These models can apply in different areas of the KYC process, and the vendor landscape is highly differentiated. KYC vendors generally fall into one of the following categories:

- Data providers.
- Data hubs/anchors for consortia.
- Entity resolution specialists.
- Workflow specialists.
- Packaged KYC providers.
- Providers of enterprise financial crime solutions.

Faced with a complex market, FIs must carefully select the KYC components that suit their needs. They must also determine how to implement their chosen system – will they integrate the components themselves, contract an implementation firm to stitch it together for them, or choose an out-of-the-box KYC/financial crime solution? To ensure they make the right choices and meet their objectives, FIs must carefully consider the nuances of their KYC requirements and the offerings available.

Our recommendations for KYC vendors include:

- **Develop services partnerships**. Due to FIs' use of implementation partners, component vendors should ensure they build the links that put them on major consultancies' radar screens when searching for new solutions in their respective KYC systems.
- **Improve systems integration**. In the same vein, vendors should bolster their solutions' capacity to work seamlessly with other KYC components, as well as core banking systems. This will strengthen FIs' KYC workflow and boost their solutions' appeal to FIs and implementation partners.
- **Deepen services offerings**. Work to provide better services – like rules suggestions – within their KYC solution. For example, offer solution extensions that interface with external services such as Dun & Bradstreet for profile enrichment.
- **Offer proof points**. Assure FIs and implementation partners of their solutions' strengths now that systems are able to hit the targets for false positives reductions and onboarding times that previously proved unattainable.

Demand-side takeaways

KYC is the process by which FIs identify customers and assess the risk they might pose. At its heart, the first step in KYC is a problem of data validation, with two main questions to answer:

- How can an FI ensure that a prospective customer – whether an individual or a firm – is who they say they are?
- Having established the customer's identity, how can they assess the risk – of regulatory infringement or reputational damage – that doing business with that customer presents?

People power – and cost

In order to perform the requisite checks while at the same time keep up with demands for rapid processing, the wage bills for FIs' KYC functions have ballooned. In addition, the more changes a system incorporates – like adding functionality to assess a person's social media profile or examine a firm's annual reports – the more tailored configuration and training is required to manage the moving parts. Manual – and often menial – tasks form the backbone of today's KYC processes, particularly at smaller FIs with lower budgets.

Beyond the complexity of systems, staff numbers are inflated further by regulatory divergence. Simply put, one centralized KYC function is not enough if regulatory requirements vary wildly across jurisdictions. Instead, FIs often have multiple KYC teams serving different countries or regions, to try and improve workers' efficiency by improving their familiarity with different regulations.

KYC analysts are being tasked with investigating networks beyond the FI's immediate relationships. FIs' growing interest in KY3P processes has also heaped yet more work on their compliance departments, pushing KYC staff counts still higher. FIs want to understand who their customers may be selling goods or services to, or providing finance to – though the bank's counterparty might carry relatively little risk, it may be transacting with sanctioned entities. FIs have become more interested in preventing the possible damage to their reputations implied by having an indirect relationship with an unsavory entity. Greater data availability has enabled FIs to map out these often murky ties. For example, the violation of export controls on military technology – whether perpetrated knowingly or not – carries severe

penalties. And if an FI's customer is hit with a large fine, the FI could be at greater risk of providing finance to or relying on deposited funds from that firm, raising the counterparty's credit risk in the process.

Services stepping up

Facing a regulatory mountain of watchlists and business demands for more rapid onboarding, KYC departments threaten to grow into huge hives populated by workers engaged in repetitive drudgery. Consequently, FIs are turning to vendors that can bring staff costs under control and make the way they deal with the growing complexity of KYC investigations more efficient. Notably, rather than raw technology solutions, these offerings typically comprise services combined with systems. Despite attempts to automate the process, the capabilities of past KYC systems have often been exaggerated, and vast reductions in false positives and onboarding times have failed to materialize.

Now, KYC is seen as something vendors can help FIs do well, and those efficiency boosts – albeit reduced – can now be achieved in the form of solutions complemented by services. We believe that the proportions of expenditure on services and technology have roughly inverted, and that spending on services now comprises the bulk of expenditure on KYC projects. These services range from helping with implementation and tailoring systems to enabling membership of consortia and providing and enriching profile data on request.

Inevitably this will mean that employee numbers will be reduced. But instead of replacing their staff outright, FIs now focus on helping them become more efficient. They are looking more for a robot hand to gather and collate information for humans to review, rather than a magic box that struggles to think on its (artificial) feet.

Supply-side takeaways

New techniques and services

To address the challenges FIs now face, vendors are offering new solutions and services that aim to cut FIs' spending by reducing the number of KYC staff they employ. By lowering the number of actions that rely solely on human involvement, these new techniques aim to make KYC processes like onboarding faster and more accurate. Applied correctly they promise to:

- Help FIs ensure that potentially valuable customers are not denied service.
- Prevent the onboarding of those that may appear safe yet hide an unacceptably high level of risk.

Four solution and service models have emerged to tackle the challenges of KYC:

- Workflow automation.
- Profile enrichment.
- Consortia and data sharing.
- Entity resolution and graph analytics.

If deployed correctly, these new solutions and services for KYC promise big benefits. FIs must choose carefully when deploying new KYC systems and processes, because the vendor landscape is highly differentiated, with KYC suppliers falling into several categories:

- Data providers.
- Data hubs/consortium anchors.
- Entity resolution specialists.
- Workflow specialists.
- Packaged KYC providers.
- Enterprise financial crime providers.

FIs also face multiple choices in the way they implement a KYC system:

- **In-house build**, which may integrate components from different vendors (assuming it is not done entirely in-house). In this case an FI selects the components and suppliers that suit its requirements – an entity resolution system from one vendor, say, and a workflow engine from another – before integrating them into a custom KYC system. This option is best for specialized institutions that may require a certain entity data model or a peculiar workflow pattern.
- **Assisted implementation**, using components packaged by an implementation partner. In this case an FI selects an implementation firm that offers a 'set menu' of KYC components best suited to its needs, or which advises on systems the FI can integrate 'a la carte'.

- **Enterprise financial crime solutions with KYC as a component**. Here an FI selects a vendor to supply a full financial crime suite that includes KYC. This is especially useful if the institution already has a relationship with the vendor and uses its platform or complementary solutions.

No vendors provide market-leading capabilities for every area of the KYC process, so FIs should consider their strategy before selecting a vendor. If they have a large backlog of unresolved onboarding data, for example, it may be wise to invest in an entity resolution specialist. If they wish to establish the 'building blocks' of a system that will be expanded in future, they may wish to start with a workflow specialist, or a well-rounded enterprise financial crime risk management vendor.

2. Quadrant context

Introducing the Chartis RiskTech Quadrant®

This section of the report contains:

- The Chartis RiskTech Quadrant® for KYC solutions for 2018.
- An examination of Pega'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?

The 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 KYC 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. It 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 and FinTech quadrants 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 Research 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 Research's 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 KYC solutions, 2018

Figure 1 illustrates Chartis' view of the KYC vendor landscape, highlighting Pega's position.

Quadrant dynamics

General quadrant takeaways

The KYC quadrant comprises three broad groups, though not all vendors fit neatly into a single category:

- **Functional and regional specialists**. These vendors have capabilities and proven track records in a niche area. This focus can be functional and/or regional – from smaller, specialized entity resolution providers to vendors that specialize in serving clients in the Middle East or North America.
- **Data providers**. Another set of specialist firms, these vendors sit higher on the market potential

axis than those in the above category, due to the potential for global uptake of their solutions. The sector in which they operate is also less crowded than that for other components in the KYC operational chain.

- **Enterprise financial crime and packaged KYC vendors**. These firms are strong all-rounders in KYC, with offerings that operate either as discrete solutions or as part of broader financial crime suites. Their market potential tends to be limited by the crowded market in which they compete.

Vendor positioning in context – completeness of offering

Pega scored highly on the KYC quadrant's completeness of offering axis, as its solution offers strong workflow and customer onboarding capabilities, many of which form the basis for other vendors' KYC systems. Features include:

- Optical character recognition for customer documents.
- Information retrieval using RPA.
- Pre-built entity relationships, allowing the onboarding of related customers in parallel.

Figure 1: RiskTech Quadrant® for KYC solutions, 2018

Source: Chartis Research

The solution's employment of zero code applications further simplifies KYC analysts' workflow by allowing rapid implementation of new compliance rules. By doing so, Pega' solution is able to reuse logic across multiple components, simplifying any upgrade path. In addition, data reuse minimizes onboarding times when possible.

Despite providing 29,000 regulatory rules for nearly 60 jurisdictions, the solution's workflow remains streamlined by only exposing those rules that are relevant to a specific customer for each KYC analyst.

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

Vendor positioning in context – market potential

Pega scored highly on market penetration, because its workflow engine provides the basis for a number of other KYC vendors' solutions.

The firm's extensive partnerships with companies such as third-party data providers further boost the potential of its KYC offering, by facilitating the ingestion of third-party data.

Pega's strategy for growth also proved strong, with a business model adapted to suit large and small clients – scalable, cross-business-line implementations for the former and out-of-the-box offerings for the latter. In addition, the firm's high level of research and development spending in areas like distributed ledger technology and RPA, as well as its provision of monthly rules updates, augments a KYC solution with already strong market appeal.

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

Table 1: Completeness of offering – Pega (KYC solutions, 2018)

Completeness of offering criterion	Coverage
Entity resolution	Medium
Reporting and dashboarding	Low
KYC risk scores	High
Customer profile enrichment with additional data	Medium
Customer lifecycle management	High
Customer onboarding	High
Workflow engine	High

Source: Chartis Research

Table 2: Market potential – Pega (KYC solutions, 2018)

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

Source: Chartis Research

3. Vendor context

Overview of relevant solutions/ capabilities

Pega's offerings are used for digital automation, business process management, case management, AI, and robotics. Its KYC and Client Lifecycle Management (CLM) solutions employ technology capabilities including AI, case management, rules and process management.

Table 3 summarizes information about Pega and its KYC solution.

Pega KYC and CLM

Pega KYC maintains a Global Master Profile across lines of business (entities and underlying parties with pre-built dependencies), products, accounts, and geographies, including related parties. It also manages complex direct/indirect and parent/child relationships to ensure re-use and efficiency in due diligence across jurisdiction and due diligence obligations.

Pega CLM, an enterprise application with features for corporate and investment banking, business banking, wealth and personal banking, provides an operating model, process backbone and case management. The solution manages all aspects of onboarding, including KYC, credit, legal, tax and

Table 3: Pega and its KYC solution

Company	Pegasystems Inc was formed in 1983 and went public in 1996. The company has more than 4,200 employees, plus 30,000 delivery professionals in its partner ecosystem.
Headquarters	Cambridge, Massachusetts, US.
Other offices	Pegasystems has 38 locations across Asia (13), Europe (12), North America (12), and South America (1).
Description	Pega provides solutions in digital automation, business process management, case management, AI, and robotics, on a single unified business platform. Its solutions in multi-channel, CLM and KYC, business rules, Customer Relationship Management (CRM) mobile solutions and adaptive analytics are designed to enable users to simplify and enhance their operations. Pega has more than 70 experts covering regulatory and onboarding within CLM and KYC business lines, and a global network of partners to deliver its applications. The financial services sector is a key focus for Pega, and alongside several hundred employees with a financial-services background, the company also partners with international consultancy firms and a global team of experts that includes former regulators and policymakers.
Solution	Pega developed its solution through collaboration with global banking clients, consulting firms and data providers. Pega CLM provides an out-of-the-box operating model, case management, rules engine and process backbone integrated with Pega KYC, and designed for multijurisdictional, multiproduct onboarding and front-to-back office transparency. Pega KYC is a rules-driven application that has been evolving for some time. The firm's KYC Regulatory Rules engine covers global regulatory rules with pre-built logic for AML/CFT, FATCA/CRS, MiFID, Dodd-Frank, EMIR[1], rules, and logic, based on factors such as booking entity, geography, line of business, percentage of ownership, customer type, and risk. Designed as an enterprise-wide solution, Pega KYC digitizes global and regional due diligence requirements, risk rating, dashboards, and complex entity management, and provides a KYC rules configuration portal.

Source: Pega

[1] *Anti-Money Laundering/Combating the Financing of Terrorism; Foreign Account Tax Compliance Act/Common Reporting Standard; Markets in Financial Instruments Directive; European Market Infrastructure Regulation.*

documentation services, with integrated reporting and front-to-back office transparency across any digital channel, prioritization and re-use.

Third-party integrations

Both applications integrate with screening providers Thomson Reuters World-Check and Equifax to screen for global sanctions, PEPs and negative media. The Equifax integration also includes ID verification, fraud verification and credit check, while the integration with ElectronicID allows identity verification through biometric matching of video images and licenses or passports. The solution also integrates with IHS Markit's kyc.com, Clarient and Avox to provide due diligence documentation and information.

Regulatory coverage

Pega KYC and CLM help firms comply with KYC due diligence requirements including: AML/CFT, FINRA 2111, US Dodd-Frank, EMIR, MiFID II, IIROC, FATCA, and CRS[2]. The solution (see Figure 2) is designed to be rapidly deployed by large global banks with zero code. Pega also recently released a permissioned KYC blockchain innovation kit.

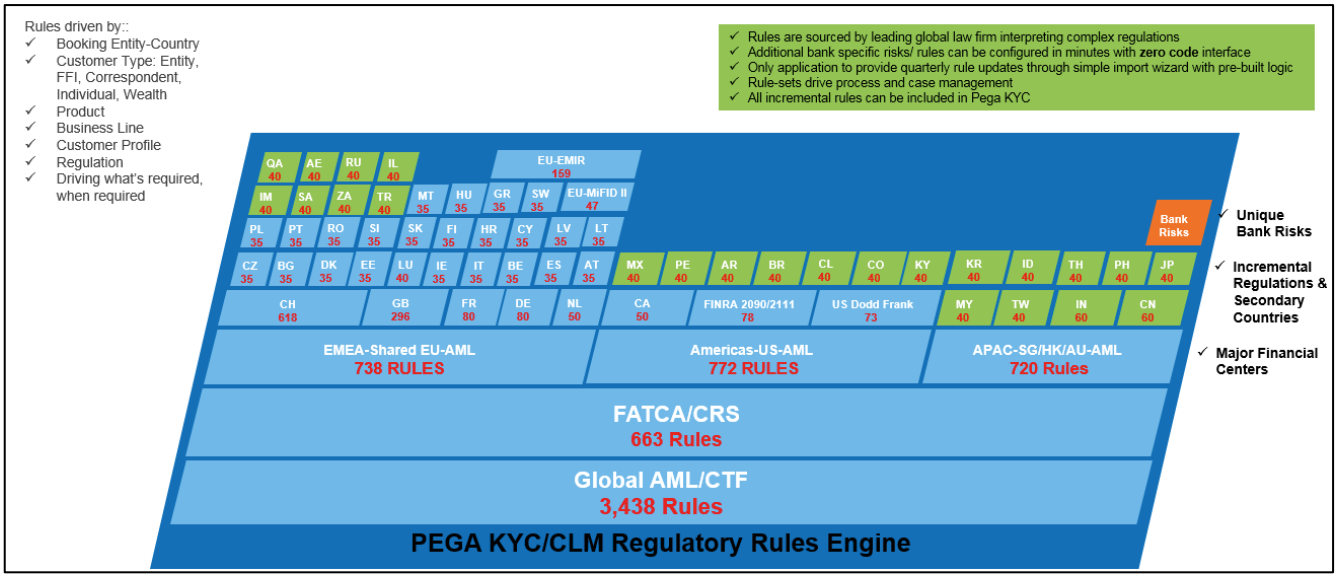
To develop and maintain out-of-the-box regulatory rulesets, Pega has partnered with an international team of lawyers, ex-regulators and policymakers.

Vendor leading practices

The key features of Pega KYC and Pega CLM are outlined below.

- Onboarding and KYC.
  - Front-to-back office onboarding and digitized KYC.
  - Cross-line-of-business application (corporate/ institutional, wealth, asset management and retail).
  - Transparency and control, front-to-back office across channels.
  - Inherent AI and robotics.
  - KYC blockchain innovation kit powered by Ethereum.
  - Speed and re-use.
    - Globally scalable.
    - Multi-jurisdictional; multi-product onboarding.
- Zero-code KYC and onboarding.
  - KYC regulatory rules engine with automated quarterly regulatory rule updates covering nearly 60 jurisdictions and 29,000 rules.

Figure 2: Pega's regulatory rules framework



Source: Pega

[2] *Financial Industry Regulatory Authority; Investment Industry Regulatory Organization of Canada*

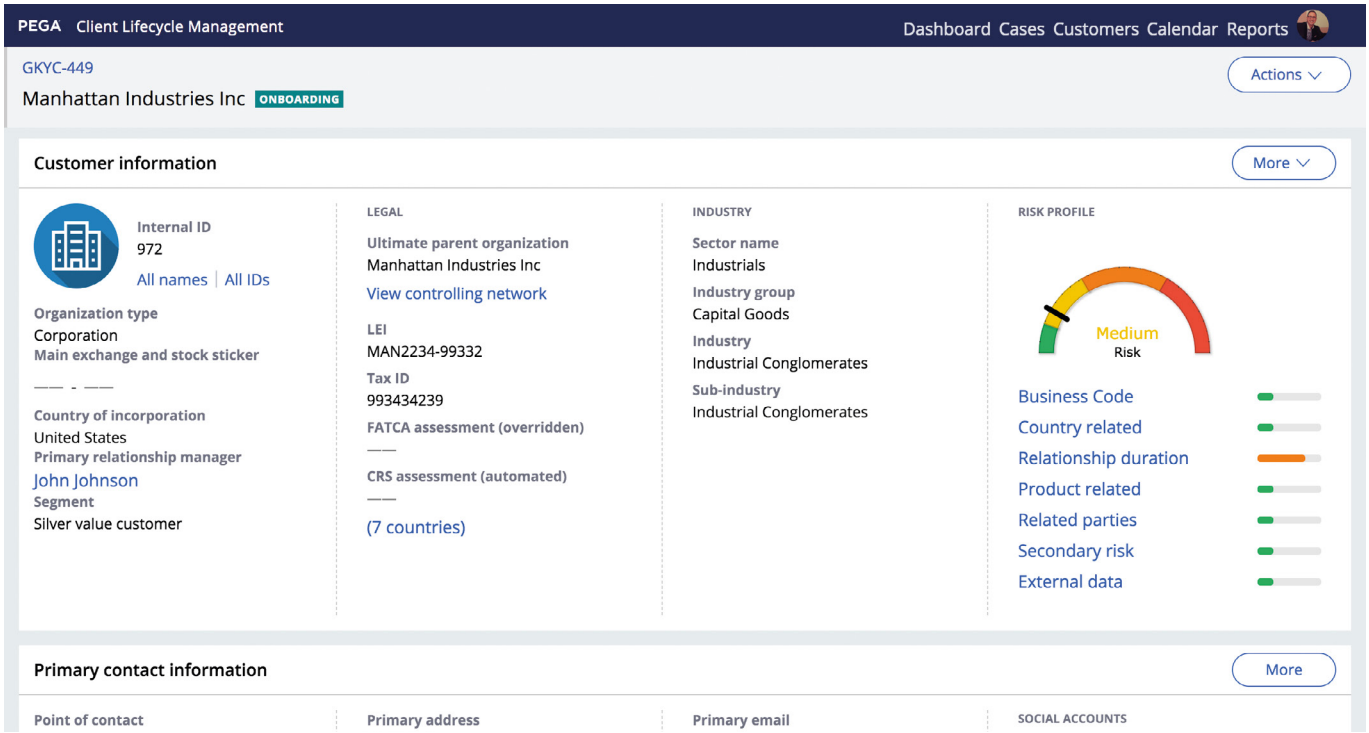
Pega KYC

- Fully integrated with Pega CLM, it provides over 29,000 pre-configured KYC due diligence rules covering AML/CFT, FATCA, CRS, EMIR, MiFID II, and Dodd Frank. Also enables global coverage of any type of KYC rules on a subscription basis.
- Regulatory rules engine.
- Regulatory rules management portal that allows for rapid zero-code updates to due diligence questions.
- Out-of-the-box functionality with automated refresh and remediation.
- Risk-rating engine that adjusts risk based on changes in information and answers to due diligence questions.
- Master customer profiles for customers and related parties that track completed due diligence, reusing it where possible.
- Out-of-the box connectors to kyc.com, Clarient, Equifax InterConnect, Thomson Reuters World-Check, Avox, Bloomberg, and ElectronicID (biometric identity verification).
- Provides overall command and control visibility and a single reusable audit repository for compliance.

Pega CLM

- A strategic application based on the Pega 7 platform, with underlying technology that is designed to scale.
- Underpinning the CLM application are unified case management, a rules engine, AI, workflow, and digital automation, allowing for parallel processing and orchestrating with full transparency in the front office.
- Pega's rules are not hard-coded – business users can change and update rules in Pega CLM and render the UI/UX rapidly with no code.
- Pega provides quarterly regulatory rule updates sourced from a global team of experts.

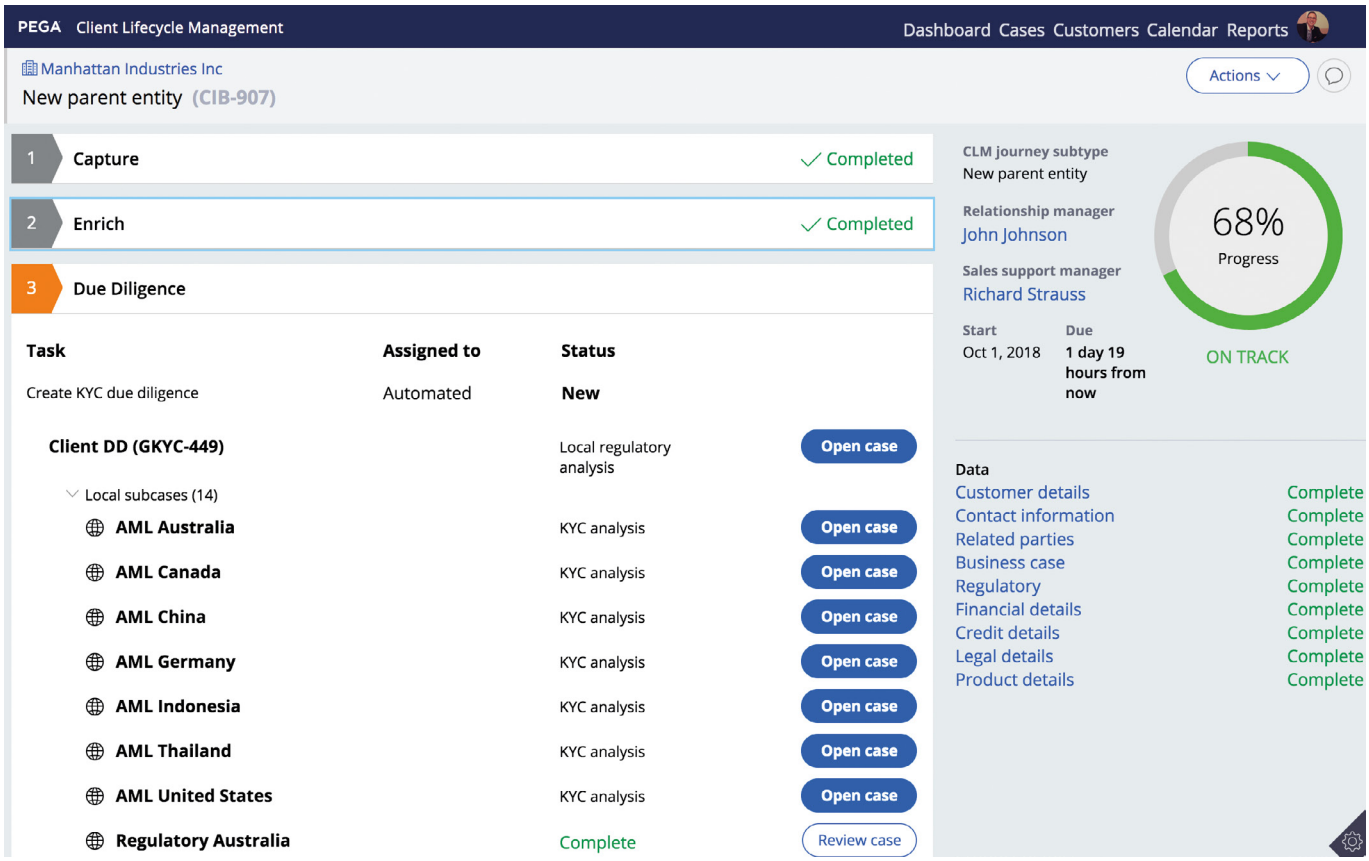
Figure 3: Pega CLM's global master view across segments



Source: Pega

- Configuration is relatively rapid; extending to new lines of business, jurisdictions and departments maximizes reuse.
- Pega offers a master folder for each entity, subsidiary and related party, including dependencies for parent/child cases (see Figures 3 and 4). This helps to ensure re-use globally, and allows banks to understand their customer relationships across jurisdictions and lines of business.
- The solution can track documentary and data requirements and coordinate several participating teams and users in parallel.
- A product database helps to speed up initial implementations and extensions to new product and service areas.
- The solution can also automatically retrieve information from other sales tools and legacy systems.

Figure 4: Pega CLM's global master view, with an emphasis on reuse and parallel processing



Source: Pega

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 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 given 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 Chartis 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 or not 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.

Selection criteria

The KYC vendor landscape is highly differentiated, with providers generally falling into one of the following categories:

- Data providers.
- Data hubs/anchors for consortia.
- Entity resolution specialists.
- Workflow specialists.
- Packaged KYC providers.
- Providers of enterprise financial crime solutions.

We selected those KYC vendors that we considered to have a significant presence in providing packaged solutions for both the retail and the wholesale side of the KYC marketplace. We took a component approach to our market analysis, looking at any vendors that provided a piece of the onboarding, monitoring and offboarding process chain. Particular consideration was given to the underlying platform and infrastructure.

Briefing process

We conducted face-to-face and/or web-based briefings with each vendor[3]. During these sessions, Chartis experts asked in-depth, challenging questions to establish the real strengths and weaknesses of each vendor. Vendors provided 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 used other third-party sources of data, such as conferences, academic and regulatory studies, and publicly available information.

[3] *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.*

Evaluation criteria

The generic evaluation criteria for each dimension are set out below. In addition to these generic criteria, Chartis utilizes domain-specific criteria relevant to each individual risk. This ensures total transparency in our methodology and allows readers to fully appreciate the rationale for our analysis. The specific criteria used for KYC solutions are shown in Table 4.

Completeness of offering

- **Depth of functionality**. The level of sophistication and amount of detailed features in the software product (e.g., advanced risk models, detailed and flexible workflow, domain-specific content). Aspects assessed include: innovative functionality, practical relevance of features, user-friendliness, flexibility, and embedded intellectual property. High scores are given to those firms that achieve an appropriate balance between sophistication and user-friendliness. In addition, functionality linking risk to performance is given a positive score.

- **Breadth of functionality**. The spectrum of requirements covered as part of an enterprise risk management system. This will vary for each subject area, but special attention will be given to functionality covering regulatory requirements, multiple risk classes, multiple asset classes, multiple business lines, and multiple user types (e.g. risk analyst, business manager, CRO, CFO, Compliance Officer). Functionality within risk management systems and integration between front-office (customer-facing) and middle/back office (compliance, supervisory and governance) risk management systems are also considered.

- **Data management and technology infrastructure**. The ability of risk management systems to interact with other systems and handle large volumes of data is considered to be very important. Data quality is often cited as a critical success factor and ease of data access, data integration, data storage, and data movement capabilities are all important factors. Particular attention is given to the use of modern data management technologies, architectures and delivery methods relevant to risk management (e.g., in-memory databases, complex event processing, component-based architectures, cloud technology, 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

Table 4: Evaluation criteria for Chartis' KYC report

Completeness of offering	Market potential
Reporting and dashboarding	Customer satisfaction
KYC risk scores	Market penetration
Customer profile enrichment with additional data	Growth strategy
Customer lifecycle management	Financials
Entity resolution	
Customer onboarding	
Workflow engine	

Source: Chartis Research

of use, are important for all risk management systems. Particular attention is given to the ability to do ad-hoc 'on-the-fly' queries (e.g., 'what-if' analysis), as well as the range of 'out of the box' risk reports and dashboards.

Market potential

- **Market penetration**. Both volume (i.e., number of customers) and value (i.e., average deal size) are considered important. Also, rates of growth relative to sector growth rates are evaluated.

- **Brand**. Brand awareness, reputation, and the ability to leverage current market position to expand horizontally (with new offerings) or vertically (into new sectors) are evaluated.

- **Momentum**. Performance over the previous 12 months is evaluated, including financial performance, new product releases, quantity and quality of contract wins, and market expansion moves.

- **Innovation**. New ideas, functionality and technologies to solve specific risk management problems are evaluated. Developing new products is only the first step in generating success. Speed to market, positioning and translation into incremental revenues are critical success factors for exploiting the new product. Chartis also evaluates business model or organizational innovation (i.e., not just product innovation).

- **Customer satisfaction**. Feedback from customers regarding after-sales support and service (e.g., training and ease of implementation), value for money (e.g., price to functionality ratio) and product updates (e.g., speed and process for keeping up to date with regulatory changes) is evaluated.

- **Sales execution**. The size and quality of the vendor's sales force, and its sales distribution channels, global presence, focus on risk management, messaging and positioning are all important factors.

- **Implementation and support**. Important factors include size and quality of implementation team, approach to software implementation, and post-sales support and training. Particular attention is given to 'rapid' implementation methodologies and 'packaged' services offerings.

- **Thought-leadership**. Business insight and understanding, new thinking, formulation and execution of best practices, and intellectual rigor are considered important by end users.

- **Financial strength and stability**. Revenue growth, profitability, sustainability and financial backing (e.g., the ratio of license to consulting revenues) are considered key to the scalability of the business model for risk technology vendors.

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 particular 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.

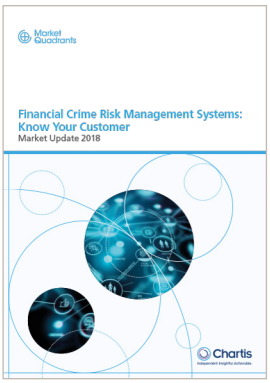
Enterprise solutions

- Enterprise solution providers typically offer risk management technology platforms, combining functionally rich risk applications with comprehensive data management, analytics and BI.
- A key differentiator in this category is the openness and flexibility of the technology architecture and a 'toolkit' approach to risk analytics and reporting, which attracts larger clients.
- Enterprise solutions are typically supported with comprehensive infrastructure and service capabilities, and best-in-class technology delivery. They also combine risk management content, data and software to provide an integrated 'one stop shop' for buyers.

Category leaders

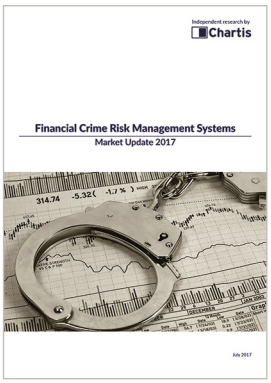
- Category leaders combine depth and breadth of functionality, technology and content with the required organizational characteristics to capture significant share in their market.
- They demonstrate a clear strategy for sustainable, profitable growth, matched with best-in-class solutions and the range 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.

5. Further reading



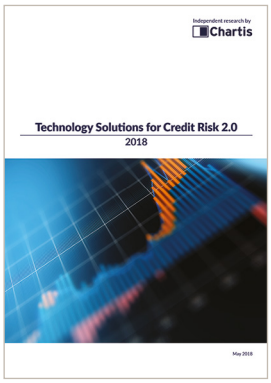
Financial Crime Risk Management Systems: Know Your Customer; Market Update 2018

RiskTech100® 2018

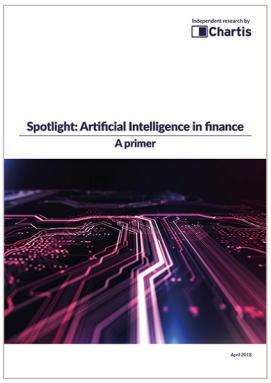


Financial Crime Risk Management Systems – Market Update 2017

Front Office Risk Management Technology 2018



Technology Solutions for Credit Risk 2.0, 2018



Spotlight on Artificial Intelligence in finance – a primer

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