Independent research by

Chartis

Vendor Highlights: Oracle

Financial Crime Risk Management Systems: Market Update 2017

October 2017

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. Executive summary

This report provides an independent evaluation and description of Oracle's leading practices and competitive position. Our analysis is based on information in the Chartis report *Financial Crime Risk Management Systems: Market Update 2017*, and the RiskTech Quadrants® for enterprise fraud technology solutions, Anti-Money Laundering (AML) solutions, Know Your Customer (KYC) systems, watchlist monitoring solutions and trader surveillance systems.

The report also includes brief coverage of:

- The main demand-side trends in this market, with an analysis of the key business and regulatory challenges.
- The supply-side dynamics, with a focus on the vendor landscape.

Against a background of more financial crime and shifting regulatory pressures, two trends are increasingly shaping Financial Institutions' (FIs') Financial Crime Risk Management (FCRM) requirements:

- Greater volumes of regulatory reports, notably Suspicious Activity Reports (SARs).
- More complex relationships, involving correspondent banking, ultimate beneficial owners, and open Application Programming Interface (API) banking.

Tackling these issues effectively will take the considered use of technology, people and process – all as budgets continue to tighten and financial crime becomes more sophisticated. Several technologies are proving useful, but three in particular – platforms/databases, Artificial Intelligence (AI) and entity resolution – are emerging as key elements in the development of effective new FCRM systems. But while these are powerful tools, FIs must recognize both their pertinence and their limitations. To make the best use of them, FIs must match them to appropriate use cases, and employ suitability analysis, backtesting and explicable methodologies.

The FCRM vendor landscape, meanwhile, is crowded, and several areas which have historically been stagnant – such as trader surveillance – are facing a significant level of disruption from new vendors, many of which are exploiting new technologies. And rather than attempting to offer multiple solutions, specialist vendors are enjoying considerable success by picking away at elements of the incumbents' technology stacks, undermining the notion of a true enterprise-wide FCRM solution.

2. Oracle: vendor highlights

Company information

Table 1 summarizes the key facts about Oracle and its KYC offering.

Table 1: Oracle – company information

Company	Oracle
Headquarters	Redwood City, California
Other offices	Oracle has offices in 38 US states, including more than five in each of California, Florida, Illinois, Massachusetts, New Jersey, New York, Ohio, Texas and Virginia. In addition, it has a global support network of contacts in 119 countries, covering a variety of languages.
Description	Founded in 1977, Oracle now has more than 800 employees dedicated to developing and selling risk products. A division of the company, Oracle Financial Services Analytical Applications (OFSAA) provides a wide range of capabilities to manage risk, compliance, financial crime, treasury, finance and the front office.
Service/offerings	The OFSAA Financial Crime and Compliance Management (FCCM) offering provides a single platform that enables FIs to implement scalable FCRM solutions quickly, with advanced analytical capabilities. The solution has modules covering data management, fraud, AML, KYC, watchlist screening and trader surveillance.

Source: Oracle

Competitive position

Figures 1 to 5 illustrate Chartis's latest view of the vendor landscape for enterprise fraud technology solutions, AML solutions, KYC systems, watchlist monitoring solutions and trader surveillance systems. In all quadrants Oracle is positioned as a Category Leader. The company rates highly for a variety of capabilities across the five FCRM areas, including real-time detection, alert management, Customer Lifecycle Management (CLM), screening technology and e-comms monitoring. Oracle also has a strong growth strategy and market penetration, coupled with significant financial strength.

The RiskTech Quadrant® is a proprietary methodology developed specifically for the risk technology marketplace. It takes into account the product and technology capabilities of vendors, as well as their organizational capabilities. Appendix A sets out the generic methodology and criteria used for the RiskTech Quadrant®.

Specifically, we have considered the following as particularly important:

Completeness of offering

Platform

- **Data management** – including the strength of the data platform, unstructured and real-time data management, validation and audit.

- **Rules engines** – including filters, claim histories, user rules and definitions, and custom rulesbuilding capabilities.

- **Analytics/modeling** – including machine learning, data mining, risk scoring, natural language processing, and model risk management.

- **Workflow engine** – including Robotic Process Automation (RPA) and case management capabilities.

- **Reporting/Business Intelligence (BI)** – including dashboards and monitoring, drill-down, tabular and graphical displays, and exporting.

- **Entity resolution and hierarchy modeling** – including network resolution, mapping and relationship building.

Financial crime risk management

- **Anti-fraud** – including screening technology, payment and internal fraud, fraud detection techniques and scenarios, and alert management.

- **AML** – including terrorist finance, blacklist management, alert management, search and transaction monitoring.

- **KYC** – including identity resolution, regulatory reporting, KYC risk scores, customer profile enrichment and customer lifecycle management.

- **Watchlist monitoring** – including screening technology, business rules, matching algorithms, and integration.

- **Trader surveillance** – including market abuse rules, e-comms monitoring, low-latency reporting, trade volume reporting, and asset coverage.

Market potential

- **Growth strategy and brand**.

- **Post-sales implementation and support** capabilities.

- **Strategy for, and investment in, continued innovation** in risk technology relating to FCRM.

- **Domain knowledge** and thought leadership in FCRM.

- **Potential value of FCRM deals** (i.e. Tier 1 clients vs. Tier 2 or Tier 3 clients).

- **Scalability of business model** (i.e. repeatable sales and delivery capabilities).

- **Geographical reach**.

- **Financial strength**.

Tables 2 to 7 show Chartis's rankings for Oracle's coverage against each of these criteria.

Figure 1: Chartis RiskTech Quadrant® for enterprise fraud technology solutions, 2017

Source: Chartis Research

Figure 2: Chartis RiskTech Quadrant® for Anti-Money Laundering (AML) solutions, 2017

Source: Chartis Research

Figure 3: RiskTech Quadrant® for Know Your Customer (KYC) systems, 2017

Key:

- *Includes client lifecycle management capabilities*
- *Does not include client lifecycle management capabilities*

Source: Chartis Research

Figure 4: RiskTech Quadrant® for watchlist monitoring solutions, 2017

Source: Chartis Research

Figure 5: RiskTech Quadrant® for trader surveillance systems, 2017

Source: Chartis Research

Table 2: Completeness of offering (enterprise fraud technology solutions) – Oracle

Completeness of offering	Coverage
Name and transaction screening	High
Payment fraud – tools and infrastructure	Medium
Internal fraud	High
Regulatory compliance reporting and controls	Medium
Real-time detection	High
Fraud detection techniques	Medium
Pre-packaged fraud rules and scenarios	Medium
Alert management	Medium

Source: Chartis Research

Table 3: Completeness of offering (AML solutions) – Oracle

Completeness of offering	Coverage
Money laundering and terrorist finance compliance	Medium
Blacklist management	Medium
Alert management	High
AML search	High
Transaction monitoring	Medium
Rules and filters	Medium

Source: Chartis Research

Table 4: Completeness of offering (KYC systems) – Oracle

Completeness of offering	Coverage
Identity resolution	Medium
Regulatory reporting	Medium
KYC risk scores	Medium
Customer profile enrichment with additional data	High
Customer lifecycle management	High
Additional due diligence support	Medium

Source: Chartis Research

Table 5: Completeness of offering (watchlist monitoring solutions) – Oracle

Completeness of offering	Coverage
Screening technology	High
Blacklist management	Medium
Business rules	High
Matching algorithms	High
Breadth of offering/number of sources supported	High

Source: Chartis Research

Table 6: Completeness of offering (trader surveillance systems) – Oracle

Completeness of offering	Coverage
Pre-packaged market abuse rules	High
E-comms monitoring	High
Low-latency reporting	Medium
Trade volume reporting	Medium
Asset coverage	Medium

Source: Chartis Research

Table 7: Market potential – Oracle

Market potential	Coverage
Financial strength	High
Post-sales implementation and support	Medium
Scalability of business model	Medium
Potential value of FCRM deals	High
Growth strategy and brand	High
Geographical reach	Medium
Domain knowledge	Medium
Current market penetration	High

Source: Chartis Research

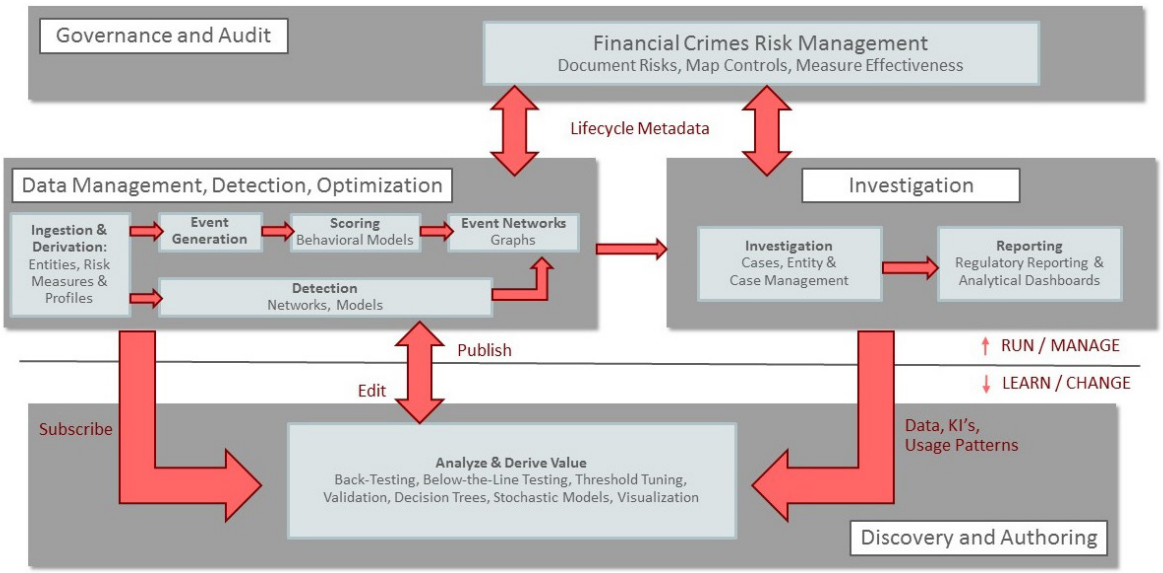
Leading practices

Oracle supplies software, hardware, engineered systems and related consulting, education and support services to more than 380,000 customers in 145 countries. Oracle Financial Services Analytical Applications (OFSAA) provides solutions for banking, capital markets and insurance, including enterprise risk, financial crime and compliance management, performance and profitability management, and customer analytics.

Oracle Financial Crime and Compliance Management is one of these solution sets. Its differentiating factors include a focus on data management, and its single underlying platform, which includes Big Data staging areas with scalable architectures. This enables FCRM solutions with high volumes of transactions to be implemented within a relatively short period of time. The analytics in the solution focus on enabling users to understand how well they are performing, with model risk management and benchmarking capabilities.

Oracle Financial Crime and Compliance Management also includes governance and audit, data management, investigation and discovery and authoring capabilities (see Figure 6).

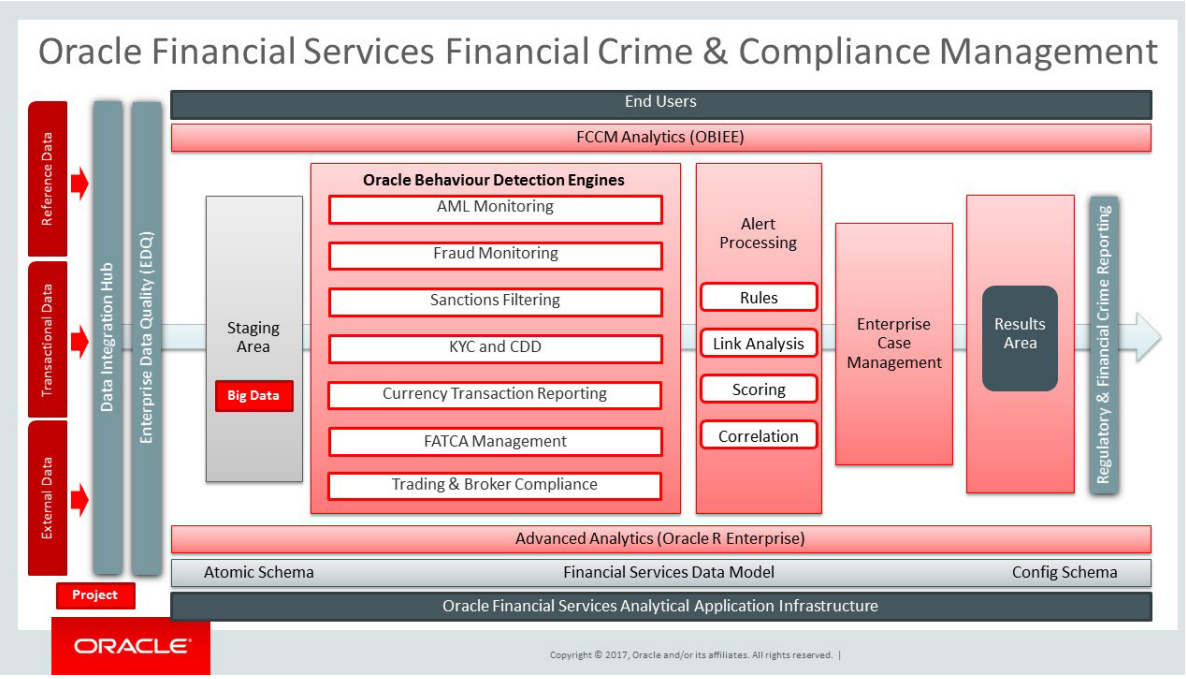
Figure 6: Oracle Financial Crime and Compliance Management – overview



Source: Oracle

The solution leverages Oracle's technology experience to provide high-volume and low-latency detection of suspicious transactions. The behavior detection application can detect complex customer, account, trader, security and household behaviors using sequence matching, rule matching and network analysis. In addition, the core behavior detection application interdicts transactions in batch or real-time processes, and feeds into the FCCM enterprise case manager (see Figure 7).

Figure 7: Oracle Financial Crime and Compliance Management – solution architecture



Source: Oracle

The solution's analytics capabilities provide users with a library of modeling techniques, and can be invoked from Oracle's Inline Processing Engine (IPE).

Oracle also bundles a highly scalable graph analytics and query engine to enable pattern detection (circular money flow, for example), detection of behavioral anomalies, entity resolution and other graph-based analytical use cases.

Oracle Financial Services Enterprise Case Management uses configurable frameworks for data integration, screening and workflows, integrating third-party systems, and capturing financials and losses to create an investigation environment which spans all behavior detection environments. The solution uses Oracle Business Intelligence to provide operational and investigative reporting capabilities via dashboards and ad-hoc reporting.

Data and access management

Oracle Financial Crime and Compliance Management can leverage the Exadata Database Machine to improve performance in high-throughput situations. Customers can also use Big Data solution architectures that encompass Oracle's Big Data offerings – Big Data Appliance, Cloudera Hadoop, Oracle NoSQL, Oracle R Enterprise, Collective Intellect and Endeca – to analyze transient and permanent customer profile data. Users can also gain immediate access to related real-time event data; this information can enable them to detect and prevent financial crime in real time using unstructured data.

Recent updates include Big Data enablement, which features data quality checks and data transformations in Hive/Spark. In addition, the FCCM banking Data Integration Hub enables users to create a 'mirror' of the banking structure to be created. In effect, this is a staging area where FCCM can be set up and tuned while other compliance processes are ongoing.

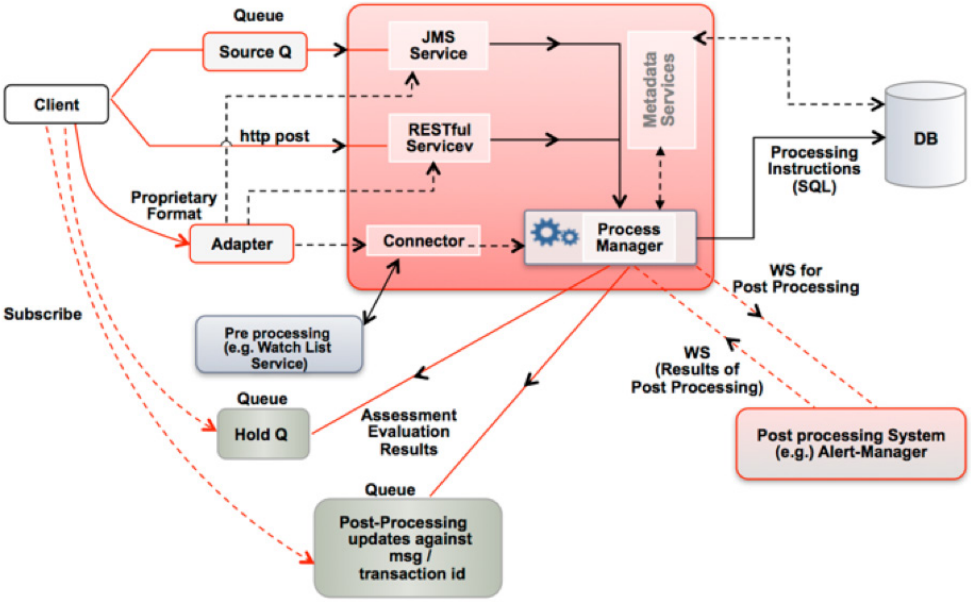
Fraud capabilities

The Oracle Financial Services Enterprise Fraud Management solution comprises the following modules and functionality:

- Oracle Financial Services Inline Processing Engine is a real-time scoring engine that can connect to different channels. It enables users to acquire data and respond with recommendations to approve or deny authorizations or transactions at the appropriate stage.
- Behavior Detection Engine enables users to execute sequence and network algorithms.
- Oracle Financial Services R Modeling Framework is a framework for performing statistical and predictive modeling on historical data with or without tagged outcomes.
- Financial Crime and Compliance Studio is an Integrated Development Environment for data scientists and scenario authors. It enables visual (graphical/tabular) exploration and interactive pattern detection of financial crime data within the Oracle Graph Analytics engine, and in Apache Spark.
- Oracle Real-Time Decisions for real-time predictive techniques, to look at new and emerging patterns without requiring historical data.
- Oracle Endeca Information Discovery is used for unstructured data analysis.
- Oracle Adaptive Access Manager provides defenses to prevent fraudulent patterns specific to particular web sessions, such as phishing, spoofing and 'man-in-the-middle' attacks.

In addition, the solution provides packaged scenarios to allow FIs to match frauds against known patterns of behavior via the Inline Processing Engine (see Figure 8). It also provides event aggregation to give concise views of potential fraud activity and identify complex behaviors in channels and systems.

Figure 8: Oracle Financial Services Inline Processing Engine – data flow



Source: Oracle

The scenarios cover first-party fraud (such as application, mortgage and loan fraud), third-party fraud (such as employee/internal fraud, identity theft and account takeover) and merchant fraud. Pre-packaged interfaces are available for a variety of channels, including:

- ATMs (including high-velocity ATM withdrawals in real-time).
- Electronic Funds Transfer at Point of Sale (EFT-POS).
- Society for Worldwide Interbank Financial Telecommunication (SWIFT).
- ACI Money Transfer System (ACI-MTS).
- Interactive Voice Response (IVR).
- Call centers.
- Branches.
- Automated Clearing House (ACH).
- Single Euro Payments Area (SEPA) in Europe.
- The Network for Electronic Transfers (NETS) in Singapore.
- Mobile and online channels.

AML capabilities

Oracle Financial Services Anti Money Laundering offers multiple scenarios designed to detect a variety of different structuring methodologies. It monitors for:

- High-risk geographies and entities.
- Hidden relationships.
- Anomalies or changes in behavior.
- Anticipatory profiling – expected vs. actual.
- Avoidance of reporting thresholds.
- Potential structuring in cash and equivalents.
- Deposits and withdrawals of mixed monetary instruments.

Oracle Financial Crime and Compliance Management takes a risk-based approach to monitoring entities for potential money laundering activity. FIs can use watchlist functionality or 'risk-rate' entities (such as accounts, customers, client banks, external entities and transactions) to enable enhanced monitoring of

those considered to pose a greater risk to the institution. The solution also shows how many alerts were captured by specific regression/analytics models, in order to enable benchmarking.

Users can incorporate both externally and internally generated lists[1] and associate a degree of risk with each. These scores are then associated with each entity on the list. Similarly, geographies can also be risk-rated, and geographical risk applied to monitoring activity. In addition, the risk associated with each transaction is calculated based on the parties, geographies, products and channels involved. Each scenario can then apply a different set of conditional thresholds so that entities or transactions identified as high risk are monitored more closely than those that are not. These risk metrics can also be used to score or prioritize the alerts that are generated.

KYC capabilities

Oracle Financial Services Know Your Customer provides configurable risk models that evaluate customer and account information, automatically cross-reference industry and internal watchlists, and validate information against independent reliable information. Oracle Financial Services Know Your Customer leverages the data collected when clients open accounts to calculate risk profiles for each account based on user-configurable risk models.

Risk models evaluate customer and account information (such as geography, account/product type, customer type and relationship). Different customer risk models exist for individual, joint, corporation and correspondent bank customers. In addition, Oracle Financial Services Know Your Customer risk models consider Ultimate Beneficial Ownership when calculating risk for a legal entity.

The customer risk calculation includes watchlist matching (including Office of Foreign Assets Control [OFAC] and PEPs); the solution can also accept lists from any public or private source. Oracle Financial Services Know Your Customer uses 'fuzzy' name matching and risk lists to identify entities and accounts considered a risk to the firm. Oracle Financial Services Know Your Customer fuzzy name matching enables users to resolve different references for persons or organizations.

The solution uses interfaces to integrate with industry-standard services, to verify identifying information against public and private sources, and to retrieve potentially negative news about clients and counterparties.

Oracle Financial Services Know Your Customer supports Ongoing Due Diligence through periodic re-reviews, as well as automated accelerated re-reviews based on changes in customer information, customer AML behaviors and/or client changes to risk-rating criteria.

Watchlist screening

Oracle Financial Services Customer Screening leverages the matching and data management capabilities of the Oracle Enterprise Data Quality platform. Its capabilities include national, regional and global sanctions and watchlists, including those from governments, Her Majesty's Treasury, OFAC and Dow Jones. Customers' own blacklists can also be included, and pre-configured connectors can be imported. The solution contains jurisdictional coverage for over 100 countries.

Using the watchlist capability, clients can associate a degree of risk (i.e. a watchlist) or trust (i.e. an exclusion list) with any entity, account or geography. There are three types of watchlist:

[1] *Such as Financial Action Task Force Conditional Cash Transfers (FATF CCTs), Previous Suspicious Activity Report (SAR) Filed and Politically Exposed Persons (PEPs).*

- **Risk**. A list of entities suspected of being involved in money laundering, and which should be monitored more strictly (using lower thresholds, for example). Various criteria associated with the entity (such as geography) can also be used. As the risk increases, the entity is monitored more closely. Risk can also be used in scoring to help prioritize alerts once they are generated.

- **Exempted**. A list of entities that are well-known to the institution (often publicly traded companies or firms with well-known business activities and relationships), and which need not be monitored for money laundering behavior.

- **Trusted**. Recognized entities that are not known to be involved in money laundering, but which FIs should continue to monitor for these behaviors, albeit less closely (using higher thresholds, for example).

Based on this watchlist data, the solution derives risk metrics for data categories such as account, client bank, customer and geography.

Trader surveillance

The Oracle Financial Services Trading and Broker Compliance solutions support a wide variety of asset classes, including: equities, fixed-income, futures, commodities, foreign exchange, options, derivatives, mutual funds, exchange traded funds, money markets, preferred, convertibles and consumer loans. A suite of monitoring scenarios enables FIs to look for behaviors across various focal entities, such as security, employees, traders, accounts and customers. The Trading Compliance/Broker Compliance solutions come with more than 150 out-of-the-box scenarios covering areas such as insider trading, customer suitability, best execution, control room functions and employee trading. Tools are also provided to allow for custom and ad-hoc scenario creation.

Behavior detection scenarios can be configured to run across multiple asset classes or just one. Parameters allow these to be configured to address the unique needs of certain asset classes. Some scenarios are developed only to address a single asset class, as the type of monitoring or regulatory need is specific to that class.

3. Context

Demand-side analysis

Overview: the deep implications of reporting and relationships

Since our last market update (in 2016), two overarching trends have emerged in FCRM. Both will have significant implications for FIs' operations:

- A substantial increase in their reporting requirements.
- A growing need to map out their increasingly complex relationships.

For FIs, managing these efficiently and effectively can be costly and complex. Alongside pressure from regulators – and financial crime itself – processing the increasing volume, variety and velocity of the data FIs now need requires customized, cutting-edge technology. Compounding these issues is growing pressure on budgets: increasingly, FIs have to do more with less. So while they are looking to use technology to help, they must take a careful, considered approach.

Evolving technology: three emerging strands

Several developments in technology have enabled FCRM solutions to evolve, including digitalization, data mining, the growth in data science, the accessibility of Big Data technologies, novel algorithmic approaches and complex pattern detection. But three technology strands increasingly appear throughout the FCRM landscape: platforms/databases, AI and entity resolution. The three overlap: AI can inform and shape entity resolution, and powerful platforms underpin much of the work done by AI. The spread of new hardware (particularly Graphics Processing Units [GPUs]) has also enabled the evolution and adoption of AI by reducing the cost of highly accelerated machine learning tools.

These developments present an often complex array of possible technology options for FIs, which are under pressure to implement cutting-edge solutions on increasingly tight budgets. Crucially, however, what constitutes 'cutting edge' depends on the use case. The Hadoop and Spark stack, for example, provides an entry point for a 'next-generation' FCRM system, with a fully featured stack available for rapid processing of unstructured data. But it is not necessarily the 'best' tool for every situation: many emerging technologies (such as machine learning, topological data analysis, graph and network analysis and evolutionary algorithms) work best with array-oriented data. FIs must evaluate the level to which different vendors have implemented their data architecture and aligned it with their individual analytical focus.

KYC: Ultimate Beneficial Ownership

Evolution in KYC has been driven mainly by UBO and relationship management, as FIs have had to provide more granular details about counterparties (and potentially *their* counterparties). FIs are also aiming to reduce the time and costs involved in on-boarding processes. More regulation and more complex data have lengthened the time taken to on-board clients and counterparties, which may prevent clients from banking with a given institution, or even in a specific region. In September 2016, for example, the Hong Kong Monetary Authority issued a company circular, warning against the potential negative effects of overly stringent on-boarding and Customer Due Diligence (CDD) processes.[2]

[2] ***http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20160908e1.pdf***

Customer Lifecycle Management/KYC+

A consequence of more complex relationship management has been the ongoing development of CLM. This is a more holistic version of KYC that covers clients from on-boarding to off-boarding, and which can be used to provide detailed descriptions of FIs' relationships with their counterparties.

So far CLM systems have often been delivered with a retail banking perspective. As such, they tend to focus more on capturing relatively simple relationships between clients: each customer is captured as a single entity and then the same 'rules' and properties are applied to it as they would be to any other entity. This has under-served merchant banks in particular, which have fewer customers but far more complex relationships – normally they have been compelled to use repurposed retail KYC systems, which are not fit for purpose.

Now, however, the CLM process is increasingly required to map more complex relationships, and to provide more information over the course of the customer lifecycle – including tax reform, global derivatives reform and data regulations. Notably, a number of vendors now offer specific, dedicated CLM solutions. These can provide a more holistic view of a wider array of clients, enabling FIs to score their risks more effectively and capture more detailed information about their relationships.

Supply-side analysis

Overview

In their new implementations, FIs' focus is shifting from compliance to saving costs: they are increasingly prioritizing ease of integration, rapid implementation times and employee efficiency. Unwinding the complex knot of fraud, AML, KYC and watchlist monitoring systems has been difficult for many FIs: their systems must maintain business-as-usual processes while they implement upgrades, and the often radical work involved in integrating systems can make this difficult. Consequently, there has been a renewed focus on managing the issues at the top of the technology stack (i.e. workflow and RPA enhancements to improve efficiency) and the bottom (i.e. data management, validation and audit processes, to improve data quality).

FIs are also emphasizing vendors' specific strengths. They want best-of-breed capabilities in all areas of their FCRM, and incumbent vendors and challengers are being forced to rely on their key competencies. As FIs increasingly mix and match to get the best FCRM solution, weaker areas in larger vendors' solutions risk being exposed by specialist providers.

A second potential threat to incumbent vendors is the arrival of technology vendors from commercial/non-financial areas, which have spotted the opportunity to capitalize on FIs' latest round of regulatory requirements. These vendors often have deep experience in specific technology areas (GRC or workflow engine capabilities, for example) and sizable reserves of cash with which to invest.

How vendors are differentiating themselves

The two key challenges facing FIs are large volumes of reports, and tracking and mapping increasingly complex relationships. Vendors are attempting to address these challenges by incorporating the following elements into their solutions:

- **Resources** (i.e. libraries, data and blacklists). These are rich data sets, including hundreds of millions of consumer entities, business entities and customer transaction records.

- **Advanced analytics** (statistical modeling, or AI). Some vendors provide powerful tools for mapping out entities and relationships. Data lineage management, from staging through to management, is increasingly important. Data mining (such as topographical analysis) is being used to provide an initial 'flashlight' to help FIs determine where to look in complex data sets, and to uncover fraud or segment data sets more effectively.

  FIs are prioritizing explicable advanced analytics with benchmarking and tuning capabilities. Most vendors have developed some machine-learning capabilities but those that can benchmark, tune and back-test their algorithms can demonstrate their effectiveness more easily to stakeholders and regulators. Some vendors provide the capability to benchmark model risk within their analytics, ensuring that processes are up-to-date and validated. This has become particularly relevant since the OCC released its Supervisory Guidance on Model Risk Management.[3]

- The **underlying technology** (databases and platforms). These include use-case-specific platforms, which incorporate time-series, columnar and Big Data databases. Some vendors offer systems optimized specifically to interact with core banking systems. This provides a limited user base, but one optimized to a specific application. Workflow and RPA tools are increasingly being used to reduce costs in implementations.

Of the three technology areas that underpin vendors' offerings, the underlying technology is the most significant differentiator for leading players. This is also the route by which a number of new vendors are entering the FCRM marketplace.

The resources available to vendors (i.e. databases of relationships and counterparties, or rules libraries) also provide a reliable differentiator – many vendors have painstakingly built up their resources over a period of many years, and it will be difficult for others to replicate them.

Analytics, however, will provide less differentiation for vendors over time, for two reasons:

- The increasing availability of cheap advanced analytics (the proliferation of open-source machine learning, for example).

- The difficulty in effectively benchmarking advanced analytics, and proving that techniques such as neural networks or forests of trees offer explicable, verifiable advantages over rules-based systems.

[3] ***https://www.occ.treas.gov/news-issuances/bulletins/2011/bulletin-2011-12a.pdf***

4. Appendix A: RiskTech Quadrant® methodology

Chartis is a research and advisory firm that provides technology and business advice to the global risk management industry. Chartis provides independent market intelligence regarding market dynamics, regulatory trends, technology trends, best practices, competitive landscapes, market sizes, expenditure priorities, and mergers and acquisitions. Chartis's RiskTech Quadrant® reports are written by experienced analysts with hands-on experience of selecting, developing, and implementing risk management systems for a variety of international companies in a range of industries including banking, insurance, capital markets, energy, and the public sector.

Chartis's research clients include leading financial services firms and Fortune 500 companies, leading consulting firms, and risk technology vendors. The risk technology vendors that are evaluated in the RiskTech Quadrant® reports can be Chartis clients or firms with whom Chartis has no relationship. Chartis evaluates all risk technology vendors using consistent and objective criteria, regardless of whether or not they are a Chartis client.

Where possible, risk technology vendors are given the opportunity to correct factual errors prior to publication, but cannot influence Chartis's opinion. Risk technology vendors cannot purchase or influence positive exposure. Chartis adheres to the highest standards of governance, independence, and ethics.

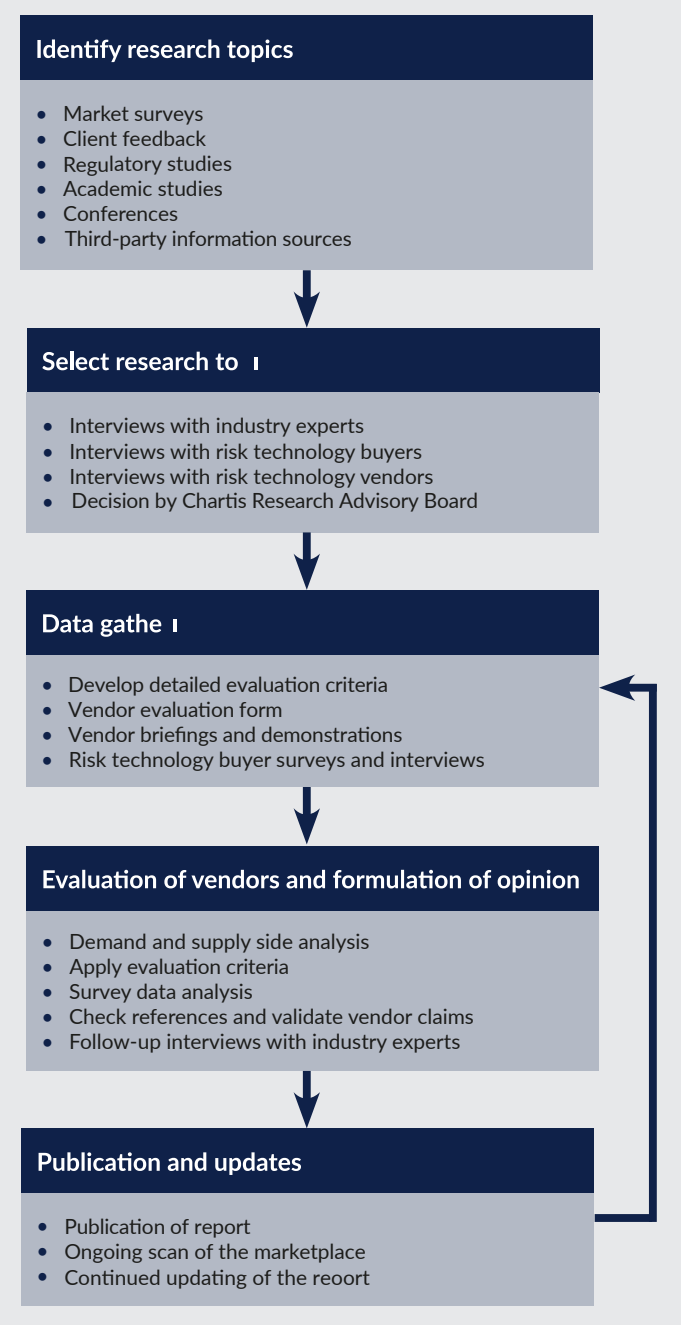
Inclusion in the RiskTech Quadrant®

Chartis seeks to include risk technology vendors that have a significant presence in a given target market. The significance may be due to market penetration (e.g. large client-base) or innovative solutions. Chartis does not give preference to its own clients and does not request compensation for inclusion in a RiskTech Quadrant® report. Chartis utilizes detailed and domain-specific 'vendor evaluation forms' and briefing sessions to collect information about each vendor. If a vendor chooses not to respond to a Chartis vendor evaluation form, Chartis may still include the vendor in the report. Should this happen, Chartis will base its opinion on direct data collated from risk technology buyers and users, and from publicly available sources.

Research process

The findings and analyses in the RiskTech Quadrant® reports reflect our analysts' considered opinions, along with research into market trends, participants, expenditure patterns, and best practices. The research lifecycle usually takes several months, and the analysis is validated through several phases of independent verification. Figure 9 describes the research process.

Figure 9: RiskTech Quadrant® research process



Source: Chartis Research

Chartis typically uses a combination of sources to gather market intelligence. These include (but are not limited to):

- **Chartis vendor evaluation forms.** A detailed set of questions covering functional and non-functional aspects of vendor solutions, as well as organizational and market factors. Chartis's vendor evaluation forms are based on practitioner level expertise and input from real-life risk technology projects, implementations, and requirements analysis.

- **Risk technology user surveys.** As part of its ongoing research cycle, Chartis systematically surveys risk technology users and buyers, eliciting feedback on various risk technology vendors, satisfaction levels, and preferences.

- **Interviews with subject matter experts.** Once a research domain has been selected, Chartis undertakes comprehensive interviews and briefing sessions with leading industry experts, academics, and consultants on the specific domain to provide deep insight into market trends, vendor solutions, and evaluation criteria.

- **Customer reference checks.** These are telephone and/or email checks with named customers of selected vendors to validate strengths and weaknesses, and to assess post-sales satisfaction levels.

- **Vendor briefing sessions.** These are face-to-face and/or web-based briefings and product demonstrations by risk technology vendors. During these sessions, Chartis experts ask in depth, challenging questions to establish the real strengths and weaknesses of each vendor.

- **Other third-party sources.** In addition to the above, Chartis uses other third-party sources of information such as conferences, academic and regulatory studies, and collaboration with leading consulting firms and industry associations.

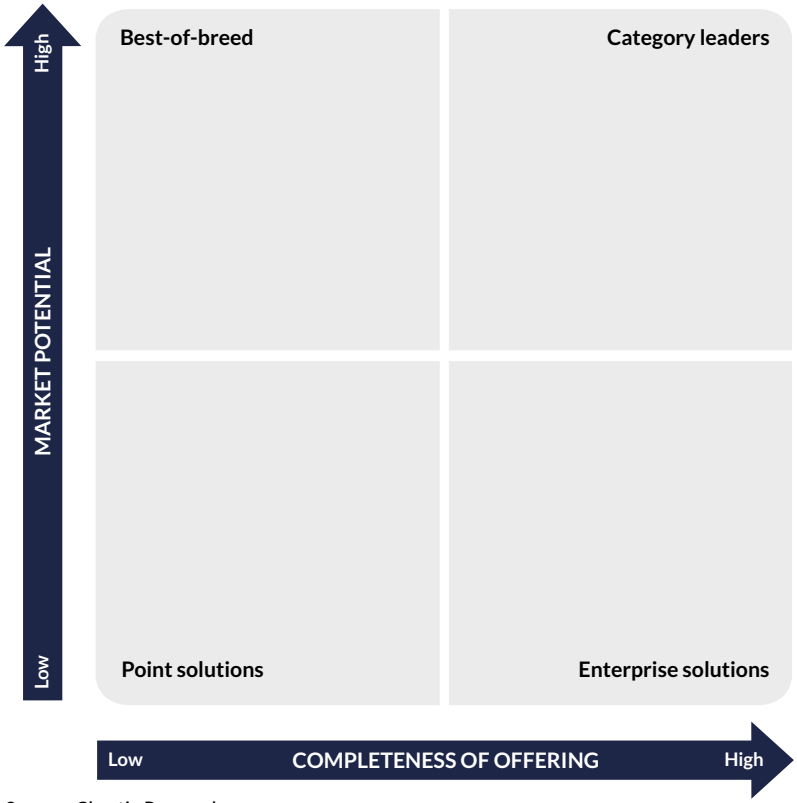
Evaluation criteria

The RiskTech Quadrant® (see Figure 10) evaluates vendors on two key dimensions:

1. Completeness of offering

2. Market potential

Figure 10: RiskTech Quadrant®



Source: Chartis Research

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

Completeness of offering

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

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

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

- **Risk analytics.** The computational power of the core system, the ability to analyze large amounts of complex data in a timely manner (where relevant in real time), and the ability to improve analytical performance are all important factors. Particular attention is given to the difference between 'risk' analytics and standard 'business' analytics. Risk analysis requires such capabilities as non-linear calculations, predictive modeling, simulations, scenario analysis, etc.

- **Reporting and presentation layer.** The ability to present information in a timely manner, the quality and flexibility of reporting tools, and ease of use are important for all risk management systems. Particular attention is given to the ability to do ad-hoc 'on-the-fly' queries (e.g. what-if-analysis), as well as the range of 'out-of-the-box' risk reports and dashboards.

Market potential

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

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

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

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

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

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

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

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

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

Quadrant descriptions

Point solutions. Providers of point solutions focus on a relatively small number (typically two or three) of component technology capabilities. These vendors meet a very important need in the risk technology market by solving specific risk management problems with domain-specific software applications and technologies. Point solution providers also provide a strong engine for innovation as their deep focus on relatively narrow subject areas generates thought leadership and intellectual capital. These vendors often have gaps relating to the broader enterprise risk management functionality and do not have the integrated data management, analytics, and business intelligence capabilities found in enterprise technology platforms. Furthermore, these vendors have not yet developed the organizational characteristics for capturing significant market share. Their growth is often constrained by lack of financial and human resources, or relatively weak sales and marketing execution.

Best-of-breed. Providers of best-of-breed solutions have best-in-class point solution capabilities together with the organizational characteristics to capture significant market share in their chosen target markets. Providers of best-of-breed solutions usually have a growing client base, superior sales and marketing execution, and a clear strategy for sustainable profitable growth. Best-of-breed solution providers can also demonstrate a healthy rate of investment in research and development, and have specific product or 'go-to-market' capabilities that give them a competitive advantage. Best-of-breed solution vendors have depth of functionality, but lack the breadth of technology and functionality required to provide an integrated enterprise-wide risk management system. Best-of-breed solutions are often considered as a subset of more comprehensive risk technology architecture and are required to co-exist with other third-party technologies or in-house systems to provide an integrated solution to a given risk management problem.

Enterprise solutions. Enterprise solution providers have a clear strategy and vision for providing risk management technology platforms. They are characterized by the depth and breadth of their technology capabilities, combining functionally rich risk applications with comprehensive data management, risk analytics, and business intelligence technologies. A key differentiator is the openness and flexibility of their technology architecture and their 'tool-kit' approach to risk analytics and reporting. Enterprise solution providers support their technology solutions with comprehensive infrastructure and service capabilities, ensuring best-in-class technology delivery. Moreover, enterprise solution providers have clear strategies for combining risk management content and data with their risk management software to provide an integrated 'one-stop-shop' for risk technology buyers.

Category leaders. Category leaders are risk technology vendors that have the necessary depth and breadth of functionality, technology, and content, combined with the organizational characteristics to capture significant market share by volume and value. Category leaders can demonstrate a clear strategy for sustainable, profitable growth, matched with best-in-class solutions. Category leaders also have the range and diversity of offerings, sector coverage, and financial strength to be able to absorb demand volatility in specific industry sectors or geographic regions. These vendors benefit from strong brand awareness, a global reach, and strong alliance strategies with leading consulting firms and systems integrators. Category leaders can also demonstrate an appetite for ongoing investment in innovation, often matched by deep pockets and a strong financial performance. Ultimately, category leaders combine deep domain knowledge in various risk topics with deep technology assets and capabilities. They can demonstrate this by addressing the needs of very large clients with complex risk management and technology requirements, as well as addressing the needs of smaller clients with standardized requirements looking for integrated solutions from a single vendor.

5. How to use research and services from Chartis

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

For risk technology buyers

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

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

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

Our vendor selection services include:

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

For risk technology vendors

Strategy

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

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

Thought leadership

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

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

6. Further reading

- *Financial Crime Risk Management Systems: Market Update 2016*
- *Data Integrity and Control Solutions in Financial Services 2016*
- *RiskTech100® 2017*
- *Enterprise GRC Solutions: Market Update 2017*
- *Spotlight on Conduct Risk Management*
- *Spotlight on Trade Surveillance in Energy Trading*

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