Financial Crime Risk Management Systems
Oracle Vendor Highlights
2014
About Chartis

Chartis is the leading provider of research and analysis covering the global market for risk management technology. Our goal is to support enterprises seeking to optimize business performance through better risk management, corporate governance and compliance. We help clients make informed technology and business decisions by providing in-depth analysis and actionable advice on the broad spectrum of risk and compliance technology offerings. 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
- Insurance risk
- Regulatory requirements including Basel 2, Basel 3, Dodd-Frank, EMIR and Solvency II

Chartis is solely focused on risk and compliance technology giving it significant advantage over generic market analysts.

Chartis 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.

Chartis Research is authorized and regulated in the United Kingdom by the Financial Conduct Authority (FCA) to provide investment advice.

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


© Copyright Chartis Research Ltd 2015. All Rights Reserved.

No part of this publication may be reproduced, adapted, stored in a retrieval system or transmitted in any form by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of Chartis Research Ltd.

The facts of this report are believed to be correct at the time of publication but cannot be guaranteed.

Please note that the findings, conclusions and recommendations that Chartis Research delivers will be based on information gathered in good faith, whose accuracy we cannot guarantee. Chartis Research accepts no liability whatever for actions taken based on any information that may subsequently prove to be incorrect or errors in our analysis. See Chartis “Terms of Use” on www.chartis-research.com.

RiskTech100®, RiskTech Quadrant® and The Risk Enabled Enterprise® are Registered Trade Marks of Chartis Research Limited.

Unauthorized use of Chartis’s name and trademarks is strictly prohibited and subject to legal penalties.
# Table of contents

1- Executive Summary ..................................................................................................................................5
2- Demand-side analysis ............................................................................................................................ 7
3- Leading practices from Oracle ............................................................................................................. 20
4- Supply-side analysis ............................................................................................................................. 27
5- Appendix A – RiskTech Quadrant® methodology .................................................................................. 34
6- How to use research and services from Chartis .................................................................................. 40
7. Further reading ........................................................................................................................................... 42
List of figures and tables

Figure 1: Financial crime risk management priorities .................................................................9
Figure 2: Customer-centric controls ..........................................................................................14
Figure 3: Anti-fraud and AML integration .....................................................................................17
Figure 4: Current FCRM processes ............................................................................................18
Figure 5: Important challenges to successful FCRM .................................................................19
Figure 6: Oracle financial crime and compliance management ..................................................20
Figure 7: Financial crime compliance management .................................................................21
Figure 8: Oracle analytical applications .....................................................................................21
Figure 9: Oracle Financial Services fraud management .............................................................23
Figure 10: Oracle Financial Services Inline Processing Engine ...................................................24
Figure 11: RiskTech Quadrant® for enterprise fraud technology solutions 2014 ......................30
Figure 12: RiskTech Quadrant® for AML and transaction monitoring solutions 2014 ............31
Figure 13: RiskTech Quadrant® for KYC and client on-boarding solutions 2014 .......................32
Figure 14: RiskTech Quadrant® for watch-list monitoring solutions 2014 ...............................33
Figure 15: Chartis RiskTech Quadrant® research process ...........................................................35
Figure 16: Chartis RiskTech Quadrant® .......................................................................................36

Table 1: Oracle’s competitive position ......................................................................................28
1- Executive Summary

In recent years financial institutions (FIs) have been subject to dramatic increases in fines for regulatory violations imposed by an ever-growing array of authorities.

As such, FIs need to be prepared to be scrutinized by the regulators in every country and region in which they have a presence. The most stringent compliance demands are occurring in the US, from the twin prongs of both federal and state regulators. The UK has been the second largest collector of fines. In addition, FIs are attempting to keep track of the intersections between political and regulatory risks – for example, trade sanctions in Russia and China, where regulation often shifts into high gear for geo-political reasons. This is engendering an environment in which all players in financial services, from the largest (countries) to the smallest (individual customers of FIs) are finding themselves under increased scrutiny.

However, FIs should ensure that they are not looking at financial crime from a solely regulatory perspective. With the rise of online and mobile transactions, FIs have sizable new challenges in preventing fraud and theft targeted at both themselves and their customers. The automation, anonymization and dissemination of information technology have opened the door to large numbers of potential fraudsters. This leads both to high-frequency low-cost losses, and to low-frequency but high-cost losses. FIs are facing a new breed of criminal who is familiar with their systems and structures, and can exploit them at multiple points. Meanwhile, financial crime risk management (FCRM) solutions are still largely rules-based and constructed around data silos.

The market for financial crime risk management solutions includes:

- Anti-money laundering (AML)
- Know-your-customer (KYC)
- Sanctions and watch-list monitoring
- Counter fraud (first and third party)
- Trade surveillance
- Cyber-security

These disciplines, at varying stages of maturity, are often integrated into specific risk management functions such as compliance, operational risk, credit risk, reputational risk and conduct risk. Institutions should decide whether to:

- Patch the holes in their financial crime risk management systems using point solutions; or
- Invest in a more integrated enterprise financial crime risk management platform.
Financial crime risk management systems require transparency: Regulators are no longer satisfied with black box solutions for financial crime risk management. They want to see evidence that the systems actually work, can be demonstrated and explained, and can prove they don’t discriminate based on demographics or other prohibited factors. Model risk management and model governance are an important part of these requirements for greater transparency.

Customer-focused FCRM solutions can provide business value: Increased confidence in their financial crime risk management systems has allowed FIs to raise limits while reducing false positives. They can invest in their customers with a greater degree of trust, and in turn generate more confidence from both their customers and investors.

Additional sources of information and intelligence are proving their worth: Multi-layered security, fraud and AML defenses such as geolocation, open source intelligence (OSINT) and social network analysis are providing new sources of information for building comprehensive views of customers and counterparties.

The building of holistic views and proactive financial crime risk management is key: Advanced analytics can be used to unify insight from across multiple sources, in order to build multi-dimensional views of customers and counterparties. These will allow FIs to take proactive steps to manage their financial crime risk, and potentially stop financial crimes before they occur.

With integration of risk and compliance becoming more important, FIs are looking to align their FCRM systems. The costs of breaking silos and data cleansing are proving prohibitive for most FIs. Many, especially the largest, with the most complex legacy systems, are using middleware, alignment, overlays and data abstraction layers to ameliorate costs and complexity.

This report uses Chartis’s RiskTech Quadrants® to explain the vendor landscape. The RiskTech Quadrant® uses a comprehensive methodology of in-depth independent research and a clear scoring system to explain which technology solutions meet an organization’s needs.

This report covers the leading vendors offering FCRM solutions and focuses on the key capabilities and strengths of Oracle as a category leader.
2- Demand-side analysis

Financial crime has become a growing threat for FIs, leading to a demand for improved processes, organization and technology. Regulators are implementing new measures and demanding more direct involvement by management, boards and directors in risk management and crime prevention. Technology plays a key role in detecting and preventing financial crime. It should adopt innovative tools and techniques for link analysis, predictive modeling, assisted intelligence and customer due diligence to deliver enterprise financial crime risk management solutions which can work across all channels.

This report includes the results of a 2014 global survey conducted by Chartis. Among 120 respondents:

- 90% were from financial services.
- 30% were from Europe.
- 29% were from North America.
- 23% were from the Asia-Pacific region.
- 18% were from the rest of the world.

Among these:

- 28% were tier 1 organizations.
- 25% were tier 2 organizations.
- 47% were tier 3 organizations.

Other sources of information used for this research include:

- 26 interviews with senior risk and compliance professionals active in FIs and leading consulting firms.
- Briefings by 30 financial crime technology vendors.
- Roundtable interviews and discussions with leading domain experts and practitioners at EY.
2.1. The separate areas of financial crime risk management

Financial crime risk management comes in a multitude of forms. For the purposes of this report, Chartis has chosen to look at the specific areas of:

- Anti-money laundering (AML)
- Know-your-customer (KYC)
- Sanctions and watch-list monitoring
- Counter fraud (internal and external)
- Trade surveillance
- Cyber-security

2.1.1 Anti-money laundering (AML)

Increased regulations are driving the demand for anti-money laundering technology. The establishment of international AML regulations such as the Asia/Pacific Group on Money Laundering (also known as the APG or APGML) has been fueled by international reputation risk — countries such as Thailand and Singapore are looking to shed their image as havens for criminals or tax-dodgers. Regulations with notable AML components include:

- EU 4th Money Laundering Directive Proposal and FinCEN ANPRM – focusing on beneficial owners, CDD and tax crimes
- OCC and FCA guidance for AML Model Risk Management
- FATCA (Foreign Account Tax Compliance Act) – focusing on tax transparency
- OECD Common Reporting Standards
- Sanctions Screening Violations 2013/2014
- FATF revisions in 2012

The Financial Crimes Enforcement Network (FinCEN), part of the US Treasury Department, has proposed the Cross Border Electronic Transmittal of Funds (CBETF) reporting initiative. It aims to get banks and other FIs to report on every cross-border wire transfer transaction over certain thresholds in order to detect the proceeds of criminal activity or the movement of any money that might be used to fund terrorism.
A review of financial crime and fraud in particular by the UK’s Financial Conduct Authority (FCA) highlighted the following issues:

- Lack of clear policies or procedures for dealing with trade-based money laundering
- Little or no management information on financial crime risks in trade finance
- Absence of specific crime prevention training for finance staff
- Staff failing to make appropriate enquiries about financial crime risks or to escalate suspicious transactions

AML remains one of the most important financial crime priorities for FIs (Figure 1).

**Figure 1: Financial crime risk management priorities**

**What are your organization’s Financial Crime Risk Management priorities for 2013-14?**

<table>
<thead>
<tr>
<th>Category</th>
<th>Most Urgent</th>
<th>High Priority</th>
<th>Medium Priority</th>
<th>Low Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity</td>
<td>30%</td>
<td>38%</td>
<td>27%</td>
<td>17%</td>
</tr>
<tr>
<td>Anti-Money Laundering</td>
<td>17%</td>
<td>29%</td>
<td>35%</td>
<td>14%</td>
</tr>
<tr>
<td>Know-Your-Customer (KYC)</td>
<td>5%</td>
<td>37%</td>
<td>39%</td>
<td>5%</td>
</tr>
<tr>
<td>External Fraud (First Party)</td>
<td>14%</td>
<td>21%</td>
<td>43%</td>
<td>7%</td>
</tr>
<tr>
<td>Sanctions and Watch-list Monitoring</td>
<td>7%</td>
<td>26%</td>
<td>50%</td>
<td>8%</td>
</tr>
<tr>
<td>External Fraud (Third Party)</td>
<td>8%</td>
<td>25%</td>
<td>43%</td>
<td>11%</td>
</tr>
<tr>
<td>Internal Fraud</td>
<td>11%</td>
<td>13%</td>
<td>49%</td>
<td>3%</td>
</tr>
<tr>
<td>Trade Surveillance</td>
<td>3%</td>
<td>21%</td>
<td>56%</td>
<td>3%</td>
</tr>
</tbody>
</table>

*Source: Chartis Financial Crime Global Survey*
2.1.2 Know-your-customer (KYC) and customer due diligence (CDD)

Know Your Customer (KYC) is an area of regulatory requirement which presents a significant challenge. The pressure of regulatory scrutiny and internal stakeholder expectations often leads to the deployment model selected being a manually intensive process requiring significant resource augmentation, which is prone to error and operational inefficiency. To address this, prior to ramping up a major manual operation, it is worth investing time and effort in the right planning, scoping and solution up front, including consideration of short term technology options, for example, to provide case management workflow.

Know-Your-Customer requires FIs to authenticate their customer identity and rate their risk. KYC and CDD allow FIs to focus compliance efforts on their highest risk customers. At the on-boarding stage, KYC/CDD is essentially a data problem, focused on the validation and verification of customer identity.

On-going due diligence, however, requires analytics that can monitor customer transactions to detect illegal activity. The on-boarding and on-going KYC and due diligence procedures should include risk scoring and support prioritization of investigations.

Optimized KYC systems need to seamlessly integrate throughout the end-to-end customer process framework covering on-boarding requirements, on-going risk monitoring, reporting and workflow. They also need to have open architectures to enable communication with front, middle and back office systems as well as external data services.

2.1.3 Sanctions and watch-list monitoring

FIs should continuously update watch lists such as prohibited entities, countries under UN or other sanctions and individuals on terrorist lists, Politically Exposed Persons (PEPs) or individuals sanctioned by a country, such as the 2014 US sanctions against some prominent Russians.

Firms, or specialist vendors, have to keep the lists updated and ensure low false positive and false negative rates while updating the information and applying it in real time. A major challenge for screening solutions is dealing with the number of different spellings and alphabets of names and locations for customers and entities. An over-cautious system can lead to a high false positive rate while systems that only screen for direct matches have a high false negative rate.

Within the last year, banks have been fined over $8 billion for sanctions violations. Firms should be completely aware of any and all sanctions, fraud or trade monitoring regulations, in any jurisdiction through which they conduct business. In the case of several large US settlements with foreign banks, the violations were approved at the highest levels of the banks and continued for years, often despite warnings from compliance officers and regulators. At some banks, fines have been treated as a cost of doing business, but FIs which continue to violate US laws risk losing their ability to clear USD transactions.
2.1.4 Fraud (internal and external)

The growth of internet and mobile banking is making the maintenance of security more difficult. Electronic fraud is increasing with the expansion of modern payment technology which can process large numbers of transactions at high speed across often complex business and client relationships.

As the number and sources of transactions rise, the security challenges become more complex, yet many FIs are using fraud detection methods built for a pre-Internet, pre-mobile era.

Fraud can occur within banks, the capital markets (including clearing houses) and insurance firms. Across these, it occurs under two basic dimensions:

- **First party fraud** occurs when a fraudster uses his/her own identity, or a fictitious identity to apply for credit without the intention to fulfil their payment obligations. This is sometimes considered “victimless” fraud, but the victim is the defrauded party, namely the FI in question.

- **Third party fraud** is when fraud is committed without the knowledge of another person, whose identity is used to commit the fraud. These are normally banking or insurance customers.

Within this, there are three levels of analytics, from the most simple/basic to the most complex:

- **Transaction score-carding.** Information about verified fraudulent transactions is used to build a scoring model.

- **Entity scoring.** Information is used to build up an image of an entity and assign it a risk score, based on different attributes such as age, family status, job start date and previous alerts.

- **Network scoring.** This is a process for generating fraud networks from existing data by automatically modeling relationships between entities in claims, looking at potentially suspicious connections.

Advanced fraud detection goes beyond business rules to include fraud analytics using advanced methods such as anomaly detection, predictive modeling and artificial intelligence, acquiring a holistic view of trader or entity activity.
2.1.5 Trade surveillance

Trade surveillance monitors exchange transactional data, including orders and executed trades, to look for violations such as wash trading, pre-arranged trading, accommodation trading, customer fraud, fictitious sales, price distortion and manipulation, trading ahead, trading against, and front running. The main purpose of trade surveillance is to prevent market abuse and market manipulation, which can severely damage a firm’s reputation and lead to significant losses and fines.

Regulators are increasing their focus on traders and market abuse. For FIs, complexity provides both an opportunity and a threat. Areas of particular complexity which require specific focus include:

- Markets where liquidity is fragmented across multiple venues or geographies
- Trading in derivatives and the underlying securities and commodities
- Complex structured products and foreign exchange (FX) either traded as an asset class or linked to another service, such as a custodian’s asset management
- OTC trades in unlisted stocks and bonds

The Markets in Financial Instruments Directive (MiFID) has a number of requirements which are relevant to trader surveillance, including:

- **Client categorization**: MiFID requires clients to be divided into three areas: eligible counterparties; professional clients; and retail clients, with verifiable systems of categorization and assessment.
- **Client order handling**: Requiring the capture of information when accepting client orders, and that firms act in their clients’ best interests.
- **Pre-trade transparency**: Requiring that order-matching systems must have aggregated order information systems and trade-systems available at the five “best” price levels.
- **Post-trade transparency**: Requiring firms to publish the price, volume and time of all trades in listed shares, even outside of regulated markets.
- **Best execution**: Requiring that firms take all possible steps to obtain the best possible result in the execution of an order for a client.

In Europe, the Market Abuse Directive and Market Abuse Regulation (MAD/MAR) are designed to restore confidence in the integrated European market and create greater cross-border cooperation. MAD harmonized national laws and established a common framework for the prevention of market abuse.
FIIs operating internationally have to follow and comply with these diverse rules as well as the panoply of international and domestic regulations, and adapt quickly to the complex and changing regulatory environment.

It is important to note that the drivers are internally-driven as much as they are regulatory: unauthorized trading can potentially lead to extremely large losses. Therefore, firms are not only looking at trades, but are attempting to gain a holistic view of the traders themselves. Regulators are looking more critically at trader surveillance to eliminate breaches of internal controls and policies. Given the heightened regulatory focus, firms are attempting to build a forward-looking strategy with an emphasis on preventive modeling.

### 2.1.6 Cyber-security

Regulators, responding to attacks that are often directed at multiple channels, products and systems have stepped up their requirements with regard to cyber-security and e-fraud.

The Bank of England CBEST framework requires the following:

- Access to cyber threat intelligence, ethically and legally sourced from organizations with rigorous standards
- Access to knowledgeable, skilled and competent cyber threat intelligence analysts who have a detailed understanding of the financial services sector
- Realistic penetration tests that replicate sophisticated current attacks based on cyber threat intelligence
- Standard key performance indicators that can be used to assess the maturity of the organization’s ability to detect and respond to cyber-attacks
- Access to benchmarks

Legacy information security, event log management, fraud and risk tools are, for the most part, inadequate in effectively defending against the newest cyber-attacks. These older tools, while still the backbone of many leading security architectures, lack deep insight into real-time user behavior and context to determine if what a user is doing is anomalous or normal.

Cybercriminals exploit this lack of insight and context by developing targeted strategies that bypass existing controls and protections. The result is a low rate of detection of sophisticated attacks, high on-going costs of manual review and increased exposure to threats as attacks continue to evolve.
2.2. FIs are attempting to manage indirect risks

Financial crime risk management is not only a regulatory demand, it is also important for customer security and trust. In addition to the regulatory and business costs of financial crime, FIs are also looking at managing customer and reputation risks. These risks are often referred to as secondary or indirect, yet their effects may be greater than the “primary risks”. After an American retailer revealed that 40 million account details had been stolen by hackers1, sales dropped almost as sharply as the stock price. Trust is even more important for banks than it is for retailers. A failure to maintain security could have a devastating impact on an FI’s customer base.

2.2.1. Putting the customer experience at the center

Improving the customer experience is often seen as something that conflicts with financial crime risk management. However, customer convenience and the customer experience are not the same thing. Firms are simultaneously attempting to place the customer at the center of their financial crime risk management platforms (Figure 2), and are also trying to ensure their clients’ protection while making transactions as quick and painless as possible, including mobile and internet banking.

---


---

Figure 2: Customer-centric controls

Bank / Insurer

Risk and financial controls

Tailored customer management

Quick customer transaction

Customer

Payments channels (Mobile, home, online)

Risk and financial controls
The counterpoint to the need for improved authentications and cyber-security is the need to keep customers happy with their banking experience. Part of the reason that many customer accounts are relatively insecure is that customers do not like using inconvenient or slow security features or having to remember and type out longer, but more secure passwords. They don’t like having to run a gauntlet of authentication questions or to retrieve their account numbers or security codes every time they log into their account, nor do they like having to speak to a member of staff to confirm purchases every time their bank suspects fraud.

Nonetheless, account security is also an important part of the customer experience, although they may not pay attention unless their personal security is breached. FIs must balance security and sensitivity, ensuring that their focus is not driven too far towards either the consumer’s convenience, or the security of their own systems. A security-conscious system may be difficult for customers to navigate, but one which is too light on security is potentially insecure. Similarly, this kind of approach must be borne in mind when considering measures such as counter-fraud: a highly sensitive system will pick up a number of potential fraudsters, but may also cause false positives, and adversely affect legitimate customers.

2.2.2 Reputation risk is a focus of banks in particular, but remains difficult to quantify

While firings and resignations are common among senior management in the wake of high-profile regulatory violations, the long-term reputational effects on FIs as a whole remain unclear.

To a limited extent, some regulators in the US are using reputation risk as a way to pressure some FIs to avoid unpopular clients such as payday lenders or gambling firms. On March 1, 2012, the Consumer Financial Protection Bureau (CFPB), a federal government agency, began collecting consumer complaints about bank accounts, so banks could face regulatory risk over their treatment of customers.

Banks are periodically the target of boycotts over any number of issues. Social media is changing the reputation environment, but banks are responding aggressively with their own social media capabilities. Some banks are jumping on discontent to lure away customers. Commonwealth Bank of Australia (CBA) monitors social media looking for any problems its customers are having, whilst also looking to spot customers at competing banks who are unhappy. The social media monitors will send out a note inviting them to move to CBA.

In general, firms are struggling to accurately quantify the effect that reputation has on a bank’s profitability. Unjustified subprime lending products for credit-worthy customers, hidden fees, mis-selling of insurance products — they may have an impact on how the individuals affected view the bank, but as long as the ATMs work and money gets deposited and can be withdrawn, reputation has a debatable effect on profitability. Firms must determine whether reputational risk management is merely useful, or critical.
2.3 Analytical evolution

Financial crime losses represent some of the most unadulterated losses which an FI can be subjected to. Driven by this, the evolution of analytics within financial crime, and within the fraud space in particular, has been particularly fast-moving.

2.4. Proactive financial crime risk management

The combination of advanced financial crime risk management analytics can be used to fine-tune business rules and to support real-time processes that can prevent financial crimes before they occur. This is proactive financial crime risk management, and at its core is the ability to build a holistic image of the customer and counterparties, enabling a multi-dimensional view and informing the FI of potential risks.

2.5. Software-as-a-service and hosted solutions

Financial crime risk management is moving toward software-as-a-service and hosted solutions. Larger and more complex FIs find their data and governance architectures are barriers to in-house implementations. Employing hosted solutions can bypass these hefty bureaucratic and technological walls. Smaller institutions, particularly in developing countries where IT accounts for a significant percentage of start-up costs, are finding hosted solutions to be more cost-effective.

2.6. The business case for integrated risk and compliance

As well as protecting against financially damaging attacks and regulatory fines, there are business compliance, efficiency, and cost advantages to be gained from integrating risk and compliance capabilities. In a recent Chartis survey of senior executives within FIs around the world (Figure 3), 71% of respondents agreed that there is a compelling business case for integrating some or all of their anti-fraud and AML systems into a single technology environment.
Figure 3: Anti-fraud and AML integration

Do you believe that there is a compelling business case for integrating some or all of your anti-fraud and AML systems into a single technology environment?

<table>
<thead>
<tr>
<th>Opinion</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly Agree</td>
<td>31%</td>
</tr>
<tr>
<td>Agree</td>
<td>40%</td>
</tr>
<tr>
<td>Neutral</td>
<td>26%</td>
</tr>
<tr>
<td>Disagree</td>
<td>2%</td>
</tr>
<tr>
<td>Strongly Disagree</td>
<td>2%</td>
</tr>
</tbody>
</table>

Source: Chartis Financial Crime Global Survey

A siloed approach to managing financial crime risk makes it almost impossible for FIs to spot patterns of behavior across the organization that will enable them to identify sophisticated attacks that target multiple sources. Regulators and FIs are increasingly drawing links between types of financial crime, including tracing fraud and trading violations as predicate offenses for anti-money laundering.

Opportunities for criminals to undertake multi-pronged attacks have been expanded by the explosion of new technologies that FIs have implemented, and the increase of remote banking transactions through internet and mobile channels (e.g. person-to-person payments and mobile banking apps). This has served to amplify the interconnectedness of financial crimes. For instance, most fraud crimes have some kind of money-laundering element to them, as the proceeds of fraud have to be placed back into the financial system, layered with transactions to separate the money from its source, and finally integrated, returning the money to the criminals from a seemingly legitimate source.

A key advantage of integrated risk and compliance is that it brings the personnel tackling different financial crimes and compliance initiatives closer together, to enable direct communication between teams managing fraud risk, AML and market abuse, for instance. This also helps organizations to visualize potential financial crime risks across business lines, and to build a holistic view of normal and abnormal behaviors.
2.7. The challenges of risk and compliance integration

In today’s competitive environment, the emphasis of many FIs is on cost reduction and efficiency improvements. Against this backdrop, it can be difficult to prioritize the fight against financial crime and simultaneously meet ever-increasing compliance requirements. At the same time, as with any business change process, risk and compliance integration is a complex undertaking.

The high-profile punitive fines doled out to several global FIs by regulators and national governments in the past few years have underlined the importance of investing in this area, but there are some difficult barriers to overcome.

According to the survey (Figure 4), only 12% of FIs currently have fully integrated FCRM processes based on a unified technology architecture and data model, while the vast majority still has significant hurdles to overcome to achieve this.

Figure 4: Current FCRM processes

Which of the following options best describes your current FCRM processes?

- Fully integrated processes and systems based on a unified technology architecture and data-model: 12%
- Semi-integrated processes and systems with some level of alignment and data sharing but not fully integrated: 69%
- Well formulated and communicated processes which are totally separate with little or no integration: 19%

Source: Chartis Financial Crime Global Survey

2.8 Managing data

When bringing together workflow, data and models into a common methodology, aligning analytics and workflows is essential, but FIs normally find that the vast bulk of the necessary work is in the data management.

A unified data platform that enables analysis of reliable and consistent information from across the organization will form the lynchpin of FCRM in future. This resonates with our survey respondents (Figure 5), 90% of whom cite access to internal data as an important challenge to successful FCRM.
**Figure 5: Important challenges to successful FCRM**

What do you see as your organization's most important challenges to successful FCRM?

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Very important</th>
<th>Important</th>
<th>Somewhat important</th>
<th>Not important</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access to internal data</td>
<td>45%</td>
<td>45%</td>
<td>11%</td>
<td></td>
</tr>
<tr>
<td>In-house knowledge and expertise</td>
<td>46%</td>
<td>43%</td>
<td>9%</td>
<td></td>
</tr>
<tr>
<td>Organizational culture and awareness of financial crime</td>
<td>49%</td>
<td>38%</td>
<td>13%</td>
<td></td>
</tr>
<tr>
<td>Completeness of data recorded electronically</td>
<td>36%</td>
<td>49%</td>
<td>14%</td>
<td></td>
</tr>
<tr>
<td>Detection of previously undetected fraud</td>
<td>27%</td>
<td>51%</td>
<td>20%</td>
<td></td>
</tr>
<tr>
<td>Budgets</td>
<td>24%</td>
<td>52%</td>
<td>20%</td>
<td></td>
</tr>
<tr>
<td>Investigative tools / solutions (including case management)</td>
<td>32%</td>
<td>45%</td>
<td>19%</td>
<td></td>
</tr>
<tr>
<td>Board level / senior management support</td>
<td>30%</td>
<td>46%</td>
<td>19%</td>
<td></td>
</tr>
</tbody>
</table>

*Source: Chartis Financial Crime Global Survey*
3- Leading practices from Oracle

Oracle Corporation is a global supplier of software, hardware, engineered systems and related consulting, education, and support services for more than 380,000 customers in 145 countries. Oracle Financial Services Analytical Applications provides solutions for banking, capital markets, and insurance, including enterprise risk, financial crime and compliance management, performance and profitability management, and customer analytics.

The Oracle Financial Services financial crime solution includes behavior detection, advanced analytics, an inline processing engine, enterprise case management, pre-trade approval, and energy and commodities trading compliance (Figure 6).

**Figure 6: Oracle financial crime and compliance management**

The solution aims to leverage Oracle’s technology strengths 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. The core behavior detection application can interdict transactions in batch or in real-time processes, using network analysis and pattern matching, and integrates with the Oracle operational risk solution (Figure 7).
Advanced analytics capabilities provide a library of modeling techniques and can be invoked from Oracle’s Inline Processing Engine (Figure 8).

Figure 8: Oracle analytical applications
Both unsupervised as well as supervised learning techniques are available as part of this library of modeling techniques. Oracle’s Real-Time Decisions engine is a self-learning engine that is used for optimization and recommendations for the next steps after the processing stage. The recommendations are produced based on pre-set performance goals for the system and the model continuously adapts and learns to meet the performance goals of the overall system. Advanced analytics leverages Oracle’s R Enterprise that is built on its open source statistical programming language and environment. Supervised learning techniques are applied with models deployed through Oracle’s R Enterprise. It is integrated with the database for scalability as well as Hadoop for high performance computing. The Inline Processing Engine can evaluate and assess scores on incoming transactions in real-time, near real-time or batch to take quick decisions to hold or release transactions. The advanced analytics are used to detect trends and cross-channel vulnerabilities, using pattern recognition and regression analysis, with self-learning analytics to cut false positive rates. Profiles can be built and refreshed periodically to match against transactions.

Oracle Financial Services Enterprise Case Management utilizes configurable frameworks for data integration, screen and workflows, integration of third party systems, and financials and loss capture to enable a user-friendly investigation environment. The solution leverages Oracle Business Intelligence to provide the capabilities for operational risk and loss reporting through dashboards and ad-hoc reporting.

### 3.1. Data and access management

The solution can leverage Exadata to improve performance in high throughput situations. Customers can leverage Big Data solution architectures that encompass the Oracle Big Data offerings: Big Data Appliance, Cloudera Hadoop, Oracle NoSQL, Oracle R Enterprise, Collective Intellect and Endeca, to persist and analyze both the transient and permanent customer profile data. Users can gain immediate access to related real-time event data for its customers. This information can augment and enable the detection and prevention of financial crime in real-time, utilizing unstructured data.

For cybersecurity and access management, Oracle Adaptive Access Manager performs both real-time and batch-based risk analysis on session, transaction, event and contextual data. Possible outcomes of these evaluations include alerts, blocking, risk-based challenge or custom integration actions to affect other systems. Virtual Devices can be implemented to prevent automated navigation of transaction interfaces and malware programmed to hijack user sessions post login. For example, if a PinPad is used to enter the destination account number of a transaction, malware cannot easily navigate this process and the random data entered and sent is not the actual account number so it cannot be altered for fraud.
3.2. Fraud capabilities

Oracle Financial Services Enterprise Fraud Management (OFS EFM) solution comprises the following modules and functionality:

Figure 9: Oracle Financial Services fraud management

- Oracle Financial Services Inline Processing Engine is a real-time scoring engine capable of connecting to channels and providing capabilities to acquire data and respond to the channels with a recommendation to approve or deny at transaction or authorization.

- Behavior Detection Engine provides capability to execute sequence and network algorithms.

- Oracle Financial Services Modeling Framework is a framework for performing statistical and predictive modeling on historical data with or without tagged outcomes.

- Oracle Real-Time Decisions enable predictive techniques, allowing users to look at new and emerging patterns without requiring historical data.

- Oracle Adaptive Access Manager provides the defenses to prevent fraudulent patterns specific to web sessions such as phishing, spoofing, man-in-the-middle attacks, etc.

Packaged scenarios are also provided to allow firms to match frauds against known patterns (Figure 9). They provide event aggregation for concise views of potential fraud activity, and identify complex behaviors in channels and systems.
The scenarios provide coverage of first party fraud (application fraud, mortgage fraud, loan fraud), third party fraud (employee/internal, identity theft, account takeover) and merchant fraud. Pre-packaged interfaces are available for channels such as ATM (including high-velocity ATM withdrawals in real-time), EFT-POS, SWIFT, ACI-MTS, IVR, Call Center, Branch, ACH, SEPA (Euro), NETS (Singapore), Mobile and Online.

### 3.3. Anti-money laundering capabilities

OFS AML offers multiple scenarios designed to detect a variety of different potential 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
These behaviors are monitored by many different angles including account based detection as well as Customer, Households, and External Entities.

OFS AML tracks demographic information as a part of the client’s business data. Multiple address and phone records can be managed for each customer and account separately. Normally non-financial transaction based rules will be managed through Oracle Financial Services Know Your Customer (OFS KYC); however, it can also be incorporated as a part of the behavior detection by clients if required. Any matches to these rules or scenarios will result in a KYC Case or a behavior detection alert respectively.

It is extremely important to note that OFS FCCM takes a completely risk-based approach to monitoring entities for potential money laundering activity. As such, the institution can take advantage of watch list functionality or “risk-rate” entities (i.e., accounts, customers, client banks, external entities, transactions, etc.) to facilitate enhanced monitoring of those considered to pose a greater risk to the institution. Users can incorporate both externally and internally generated lists (i.e., SDN, FATF CCTs, Previous SAR Filed, Politically Exposed People, etc.) and associate a degree of risk with each list. These scores are then associated with each entity on the list. Similarly, geographies can also be risk rated, and geographical risk brought to bear on 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.

3.4. Know-your-customer (KYC)

Oracle Financial Services Know Your Customer (OFS KYC) provides the ability for financial institutions to assess and manage the risk of their customers based on configurable risk models that evaluate customer and account information, automatically cross-reference industry, as well as internal, watch lists, and validate information against independent reliable information. OFS KYC leverages the data collected at account opening to calculate comprehensive risk profiles for each account based on firm-configurable risk models.

OFS KYC leverages the data collected at account opening to calculate comprehensive risk profiles for the customer and for each account based on firm-configurable risk models that evaluate customer and account information (e.g., geography, account/product type, customer type, relationship). Different customer risk models exist for individual, joint, corporation and correspondent bank customers.

The customer risk calculation includes watch list matching (OFAC and PEP included). OFS KYC can accept lists from any public or private source. OFS KYC uses Fuzzy Name Matching in conjunction with Risk Lists to provide a capability to identify those entities and accounts considered to pose a risk to the firm. OFS KYC Fuzzy Name Matching facilitates resolution of different name references for a person or organization.

The solution uses standard interfaces to integrate with industry standard services to verify identifying information against both public and private sources, and with industry standard services to retrieve negative news stories. These interfaces can be leveraged to retrieve verifications from Oracle’s partners, third-party vendors, or internal systems. All information retrieved is captured with the review and available for analyst review and use in risk assessment. In addition, information from additional internal or external sources can be attached to the review or maintained in enterprise document repositories and referenced/linked in OFS KYC. Oracle offers a variety of applications to cover the following authentication capabilities, which OFS KYC may leverage to deliver a full end to end solution.
3.5. Watch list screening

Oracle Watchlist Screening leverages matching and data management capabilities of the Oracle Enterprise Data Quality platform. The capability includes national, regional and global sanctions and watch lists, including government, Her Majesty’s Treasury, US Office of Foreign Asset Control, Dow Jones, and others. Customers’ own blacklists can also be included. Pre-configured connectors are available for import. The solution contains jurisdictional coverage for over 100 countries.

Within the watch list capability, the client can associate a degree of risk (i.e., watch list) or trust (i.e., exclusion list) with any entity, account, or geography. There are 3 types of Watch Lists:

- **Risk**: Entities suspected of being involved in money laundering and that should be monitored more strictly (i.e., use lesser thresholds). Various criteria associated with the entity such as geography can also be used to associate risk with an entity. As the risk increases, the entity is monitored more strictly. Risk can be used in scoring to help prioritise alerts once they are generated.

- **Exempted**: Entities that are well known to the institution (often publicly traded companies or firms with well-known business activities and relationships), and a determination has been made that they need not be monitored for money laundering behaviors.

- **Trusted**: Known entities that are not known to be involved in money laundering but who should continue to be monitored for these behaviors, but less strictly (i.e., use higher thresholds).

Based on this watch list data, the solution derives risk metrics for data categories such as Account, Client Bank, Customer and Geography.
4- Supply-side analysis

While advances in technology are creating new threats in new channels, technology is also offering FIs a greater ability to tackle financial crime. Risk management systems are now able to monitor cross-channel, in real-time, and can help firms to identify emerging risks to detect and prevent fraud and financial crime threats.

Vendors are beginning to offer consolidated, integrated solutions. While no vendor yet has a comprehensive, fully integrated financial crime risk management platform, the leading vendors all display some combination of deep analytical capabilities and proprietary data management platforms, including real-time and unstructured data management capabilities. This enables the integration of risk and finance across multiple channels, jurisdictions, lines of business and customer lifecycle stages. The most common linkages and integration opportunities are those of counter-fraud, AML, and case management. Also, a few industry-leading vendors have begun to integrate other capabilities such as efficient cyber-security.

A number of vendors continue to produce best-of-breed point solutions for areas such as watch-list filtering, transaction monitoring and cyber-security. Both comprehensive, integrated systems and point solutions have their place in financial crime risk management, particularly with respect to the size of firms.

- Tier 1 firms will combine larger data management systems with the best of breed point and out-of-the-box platforms. The largest firms are simply too organizationally and technologically complex to effectively establish enterprise-wide financial crime risk management.

- Tier 2 firms may be able to implement enterprise financial crime risk management architectures, and will be focusing on those vendors with broad integrated capabilities and common data models.

- Tier 3 and smaller firms will mostly acquire simple, out-of-the-box solutions for regulatory compliance and basic anti-fraud capabilities with a higher propensity for hosted solutions.

Vendors are beginning to offer layered data abstraction processes that bridge across silos to gain enterprise information through defined “canonical” depictions of the models and data within. This enables the end-to-end control of data, while allowing for views across the silos and application of data security rules.

Vendors are also attempting to address the dilution of expertise within the marketplace. Many FIs are struggling with expertise bottlenecks, and a dearth of highly trained FCRM professionals. The ease-of-use of solutions, including visualizations and case management, is considered to be particularly highly prized. In addition, those who have established centers of research or knowledge are considered particularly able to keep up with the rapidly changing evolution of financial crime.

Real or near-real time data management is being offered by leading vendors. High velocity internet and mobile banking require watch-list screening and transaction monitoring to be performed in real time to prevent illicit transactions. In addition, effective crime prevention requires streamlined processes, standard definitions and common rules operating through automated workflow management. These should cover multiple business and product channels.
4.1. Oracle’s competitive position

Chartis considers Oracle to be a leading vendor in the financial crime risk management market. Its position in the vendor landscape is based on our assessment of its relative strengths and weaknesses in Table 1 below. The RiskTech Quadrant® uses a comprehensive methodology of in-depth independent research and a clear scoring system to explain which technology solutions meet an organization’s needs. The RiskTech Quadrant® does not simply describe one technology solution as the best FCRM solution; it has a sophisticated ranking methodology to explain which solutions would be best for specific buyers.

<table>
<thead>
<tr>
<th>Completeness of offering</th>
<th>Details</th>
<th>Oracle capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert management</td>
<td>Including workflow, rules and filters, claim history triggers, fraud detection, predictive analysis</td>
<td>High</td>
</tr>
<tr>
<td>Case management</td>
<td>Including case analysis, creation, databases, entry, and workflow management</td>
<td>High</td>
</tr>
<tr>
<td>Security controls</td>
<td>Including knowledge databases, user rules and definitions, cyber-security, system monitoring, and audit</td>
<td>Medium</td>
</tr>
<tr>
<td>Watch-list and sanctions monitoring</td>
<td>Including business rules, false positive reductions, black list management, screening technology</td>
<td>High</td>
</tr>
<tr>
<td>Analysis of recorded data</td>
<td>Including customer identification, KYC risk scores, name screening, insider compliance, payment transactions, and event records</td>
<td>High</td>
</tr>
<tr>
<td>Reporting tools available</td>
<td>Including dashboards and monitoring, drill-down, tabular and graphical displays, and export</td>
<td>High</td>
</tr>
<tr>
<td>Advanced analytics</td>
<td>Including AI, machine learning, natural language processing, entity extraction, unstructured data analytics</td>
<td>Medium</td>
</tr>
<tr>
<td>Model risk management</td>
<td>Including model risk identification, assessment, quantification, model use, and model performance monitoring</td>
<td>High</td>
</tr>
<tr>
<td>Supporting data and metadata framework</td>
<td>The capabilities need to be underpinned by scalable, flexible data and metadata infrastructure, providing organizational hierarchies, client hierarchies and product metadata, enabling workflow, product control and reporting</td>
<td>High</td>
</tr>
<tr>
<td>Market share potential</td>
<td>Details</td>
<td>Oracle capabilities</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Growth</td>
<td>Including strategy and brand</td>
<td>Medium</td>
</tr>
<tr>
<td>Post-sales implementation</td>
<td>Including support capabilities</td>
<td>Medium</td>
</tr>
<tr>
<td>Innovation</td>
<td>Including strategy and investment</td>
<td>High</td>
</tr>
<tr>
<td>Domain knowledge</td>
<td>Including thought leadership</td>
<td>High</td>
</tr>
<tr>
<td>Potential value of financial crime risk management deals</td>
<td>Including tier 1 clients vs. tier 2 or tier 3 clients</td>
<td>Medium</td>
</tr>
<tr>
<td>Scalability of business model</td>
<td>Including repeatable sales and delivery capabilities</td>
<td>Medium</td>
</tr>
<tr>
<td>Geographical reach</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>Financial strength</td>
<td>High</td>
<td></td>
</tr>
</tbody>
</table>

4.2. RiskTech Quadrants® for financial crime risk management systems

Figures 11-14, below, describe Chartis’s view of the vendor landscape for financial crime risk management solutions. As the scope of financial crime risk management is too broad to cover accurately within a single RiskTech Quadrant®, it has been divided into four areas:

- Enterprise fraud
- AML and transaction monitoring
- KYC and client on-boarding
- Watch-list monitoring

As part of this research Chartis also considered the creation of additional RiskTech Quadrants for cyber-security, insurance fraud and trade surveillance. However, our scan of the vendor landscape showed these sub-segments to be still relatively immature (i.e. a small number of vendors and/or early-adopter product lifecycles). We aim to generate future RiskTech Quadrants for these sub-segments as the markets evolve over the next few years.

The RiskTech Quadrant® is a proprietary methodology developed specifically for the risk technology marketplace. It takes into account 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®.
Figure 11: RiskTech Quadrant® for enterprise fraud technology solutions 2014

1. Tonbeller has been acquired by FICO as of 13/01/15
Figure 12: RiskTech Quadrant® for AML and transaction monitoring solutions 2014

1. Tonbeller has been acquired by FICO as of 13/01/15
Figure 13: RiskTech Quadrant® for KYC and client on-boarding solutions 2014

1. Tonbeller has been acquired by FICO as of 13/01/15
Figure 14: RiskTech Quadrant® for watch-list monitoring solutions 2014

1. Tonbeller has been acquired by FICO as of 13/01/15
2. Includes capabilities of Accuity and FircoSoft, which were acquired by Reed Elsevier
5- Appendix A – RiskTech Quadrant® methodology

Independence

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 is authorized and regulated by the Financial Conduct Authority (FCA) in the UK for providing investment advice and 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 15, below, describes the research process.
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 on-going 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® evaluates vendors on two key dimensions (Figure 16):

- Completeness of offering
- Market potential

---

![Chartis RiskTech Quadrant®](image-url)
The generic evaluation criteria for each dimension are set out below. In addition to the generic criteria below, Chartis utilizes domain-specific criteria relevant to each individual risk. These are detailed in the individual Vendor Evaluation Forms, which are published as an appendix to each report. 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 on-going 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.
6- 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 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
7- Further reading

• Operational Risk Management Systems for Financial Services
• Data Management and BI for Risk
• Enterprise Fraud Management Solutions 2013
• Anti-Money Laundering Solutions 2013

For all of these reports see: www.chartis-research.com