Tackling financial crime through integrated risk and compliance
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.

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

© 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.
About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EY’s Financial Services advisory practice has dedicated globally integrated teams specializing in Financial Crime, Financial Crime Technology, and Information Security. We draw on deep industry knowledge and technical skills to deliver solutions in areas including Anti-Money Laundering, Know Your Customer, Sanctions, Fraud Detection, Trader/Market Surveillance and Cyber Security. Our services include risk assessment, regulatory response, target operating models, technology strategy, model development and optimization technology delivery, remediation, controls effectiveness testing and independent review.

The views reflected in this article are the views of the author and do not necessarily reflect the views of the global EY organization or its member firms.
## Contents

1. Tackling financial crime through integrated risk and compliance 5
2. About the EY contributors 15
3. How to use research and services from Chartis 16
4. Further reading 18

### List of figures and tables

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1</td>
<td>Financial intelligence unit</td>
<td>6</td>
</tr>
<tr>
<td>Figure 2</td>
<td>Anti-fraud and AML integration</td>
<td>7</td>
</tr>
<tr>
<td>Figure 3</td>
<td>Bringing together data, models and workflow into common methodologies</td>
<td>8</td>
</tr>
<tr>
<td>Figure 4</td>
<td>Current FCRM processes</td>
<td>9</td>
</tr>
<tr>
<td>Figure 5</td>
<td>Important challenges to successful FCRM</td>
<td>10</td>
</tr>
<tr>
<td>Figure 6</td>
<td>The customer life cycle</td>
<td>11</td>
</tr>
<tr>
<td>Figure 7</td>
<td>FCRM expenditure</td>
<td>13</td>
</tr>
<tr>
<td>Figure 8</td>
<td>Example target architecture for integrated financial crime risk and compliance management</td>
<td>13</td>
</tr>
</tbody>
</table>
Leading financial institutions (FIs) are rethinking their organizational structures to manage financial crime risk more effectively. The integration and alignment of risk and compliance functions will be crucial if the financial services sector is to address the broader sources of financial crime risk and tightening regulation to which it is exposed today.

FIs are becoming exposed to increasingly sophisticated techniques used by organized criminals, who target vulnerabilities that are opening up as large volumes of customers perform multiple transactions across multiple channels. Cyber threats are one part of the equation, but FIs are grappling with criminals who often target a number of different internal and external channels. In addition, they must monitor traders, sanctions and watch-lists, and deal with the proliferating numbers of smaller financial crimes, all the while managing tightened budgets.

At the same time, the sector is facing a significant compliance burden as regulation of its practices continues to tighten, and as customers and investors demand greater transparency and integrity from financial dealings. The introduction of the Foreign Account Tax Compliance Act (FATCA) in the US this year – as well as the subsequent intergovernmental agreements (IGA) to follow – is just one such signal of international intent to make FIs more accountable for risk and compliance management on behalf of their customers. In addition, the operational costs of financial crime risk management are rising: the monitoring of the multitude of channels is proving to be increasingly expensive for firms in terms of expertise and the establishment of Financial Crime Risk Management (FCRM) Systems.

There have been several recent cases of large FIs being fined by regulators and reproached in the media for failures in their anti-money laundering (AML) and sanctions monitoring controls, too. Given that such financial crime is fundamental to the operations of terrorists, drug traffickers and corrupt political regimes, FIs simply cannot afford to risk the reputational damage inflicted by such compliance failures.

The traditional silo-based approach to the management of financial crime risk and compliance – whereby separate organizational structures support individual risk types such as money laundering, card fraud or internal fraud – will no longer suffice. A disconnected set of fraud or AML platforms is less likely to stand up to attacks that cut across multiple business lines, geographies and risk types. It is for this reason that FIs are looking towards integrating their risk and compliance systems. In the long term, small incremental adjustments to systems and processes will simply not be enough.
The EY point of view: The establishment of financial intelligence units

One emerging industry trend in response to increased regulatory scrutiny is the adoption of financial intelligence units (FIU). Financial institutions are looking to establish or enhance their financial intelligence units in order to better leverage disparate sources and available internal and external intelligence to improve the effectiveness and efficiency of their financial crime risk management programs (Figure 1).

The core concepts of collation, analysis and dissemination of intelligence are highly applicable to the current environment in FIs. While the approaches to design and implementation of an FIU vary significantly across industry, FIs are recognizing the benefits of maximizing the information available for analysis and investigation along with standardizing processes across lines of business, geographies and financial crime domains (e.g., AML, fraud, bribery, corruption, sanctions, tax evasion and cybercrime). Longer term, FIU concepts encourage a more proactive stance to financial crime risk management, allowing banks to better identify and be more adaptive to emerging trends and typologies.

Figure 1: Financial intelligence unit
The business case for integrated risk and compliance

Apart from 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 2), 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.

A siloed approach to managing financial crime risk makes it almost impossible for FIs to spot patterns of behavior across the organization, which will enable them to identify sophisticated attacks that target multiple sources. Regulators and FIs are drawing links between types of financial crime. Fraud and trading violations are increasingly being regarded as predicate offenses—those offenses whose proceeds may become the subject of 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 inter-connectedness of financial crimes. For instance, most fraud crimes have some kind of money-laundering element in 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 among teams managing fraud risk, AML and market abuse, for instance. This also helps organizations visualize potential financial crime risks across business lines, and build a holistic view of normal and abnormal behaviors.

There are several examples in the industry of how FIs can obtain benefits from sharing intelligence and information from different risk and compliance silos to glean insights on financial crime risks. For example:

- Rogue trading events may have been better understood by combining views on toxic combinations of access with unauthorized trading activity for individual trades.
- More comprehensive KYC and trader surveillance information for individual broker dealer customers may have identified toxic, large-scale Ponzi schemes using floats generated by sophisticated check kiting techniques earlier.
- New human and drug trafficking typologies have benefited from sharing information between fraud and money laundering departments.
Convergence of people, processes, technology and data

Until now, most FIs have been reacting to the sector’s rapidly evolving regulatory requirements on a piecemeal basis, meaning that some of the data and technology being used to combat financial crime have been duplicated across the organization. The integration of risk and compliance is an opportunity to remove that duplication of effort, and to bring data and analytics together into a central and consistent environment.

This environment can be considered to consist of three key building blocks that must be brought together: data, models and workflows. These can be drawn together into common methodologies and processes, enabling standard operating models, and consistent analysis across risk silos, and organizational and geographical barriers (Figure 3).

In most FIs, separate business lines use individual case management databases for logging and managing risks that arise, while reporting is also done on a siloed basis. Pooling cross-organizational, cross-border data is perhaps the most important step in the integration process. An enterprise financial crime data management strategy can deliver a host of advantages, such as:

• The identification of previously unidentified patterns of behavior through linking unusual activities across risk silos, business lines and borders.
• The recognition of new threats and construction of intelligence that can be used to enhance controls in individual monitoring platforms.
• The ability to recognize the scale of impact of an attack and coordinate an appropriate response.
• The ability to enable true enterprise-wide search to facilitate internal and external requests for information.

Cost savings

Recent discussions with Tier 1 FIs have revealed that, if managed properly, the integration of multiple risk and compliance functions can deliver cost savings between 20% and 30%, as a broad estimate.

This is achieved through a combination of system and process rationalization. Creating a unified data platform will reduce the cost of ownership for a particular system, because the support and maintenance costs are shared. The integration of systems makes data management an easier task too.

Figure 3: Bringing together data, models and workflow into common methodologies

Common methodologies

Data
- Risk data can be shared across the lines of AML, fraud, sanctions monitoring, trader surveillance, and cyber security.
- Data can be shared across business lines and geographies to establish a common standard. This should take into account any potential issues with national and regional data protection laws.

Models
- Linked models can be used to build holistic views of customers.
- More efficient or specifically purposed analytics for counter-fraud or AML can be re-used and utilized to reinforce or disprove conclusions from their neighboring disciplines.

Workflow
- Workflow activities can be brought together into an enterprise-level case management system.
- A single hub can be created for investigations or action plans.
A centralized financial crime department can also provide a centralized group of investigators, cutting down on manpower and bottlenecks in expertise, and enabling more efficient investigations and reporting. This can cut down on duplication of effort, increase transparency, scalability, and agility. In the end, this can result in significant cost savings while improving risk management.

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 the 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 unified technology architecture and data model, while the vast majority still has significant hurdles to overcome to achieve this.

Breaking down silos

A more holistic approach to tackling FCRM is needed because without a centralized approach, it becomes almost impossible to join the dots in recognizing patterns of behavior associated with organized attacks.

Before getting down to the hard graft of technological integration, FIs need to ensure that their organizational structures are aligned. It is a common error to attempt to “patch up” perceived organizational gaps with technology and, in the long term, this will only serve to create yet more structural complexity.

A key issue that FIs must address is the need to align all the various efforts taken to manage financial crime risk and compliance across the organization. For example, some aspects of FCRM, such as counter-measures for internal and external fraud, are directly driven by the business case and introduced to prevent direct losses or bad debt provisions. Other aspects, however, will be driven by regulation, such as AML, FATCA and sanctions monitoring, and by indirect losses in the form of regulatory fines and brand erosion. It is vital to ensure that these different motivations for change do not

---

**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 that are totally separate with little or no integration
  - 19%

Source: Chartis financial crime global survey
lead to change processes being undertaken by isolated teams that are not working toward the aligned risk appetite of the firm. Ideally, these individual initiatives need to be managed as a portfolio with a vision for an integrated target operating model.

This process is made more challenging in larger FIs, which are inherently complex. For example, many of today’s largest financial institutions have grown through mergers and acquisitions (M&A) at some stage, which often gives rise to silos where business units in the acquired firm are not sufficiently consolidated into the new organization because of difficulties in aligning mismatched products, services, and processes.

Furthermore, FIs have not historically been strong at documenting and developing a consistent IT architecture, meaning that M&A events have also led to overlapping and complex legacy systems in many cases. In terms of FCRM systems, it may be that specific systems are dedicated to individual areas, such as check fraud, credit card fraud, and so on. In many cases, these systems and their data will need to be realigned to establish a unified FCRM platform.

At the same time, business transformations can create long-lasting misalignments in business practices and culture. In order to manage financial crime risk and compliance more effectively, firms must overcome this barrier by educating the workforce to use common methodologies when identifying and scoring risks, for instance, and to ensure that internal risk and compliance standards and taxonomies are aligned.

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), 92% of whom cite the quality of available 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?

- Access to internal data: 45% Very important, 45% Important, 11% Somewhat important, 0% Not important.
- In-house knowledge and expertise: 46% Very important, 43% Important, 9% Somewhat important, 0% Not important.
- Organizational culture and awareness of financial crime: 49% Very important, 38% Important, 13% Somewhat important, 0% Not important.
- Completeness of data recorded electronically: 36% Very important, 49% Important, 14% Somewhat important, 0% Not important.
- Detection of previously undetected fraud: 27% Very important, 51% Important, 20% Somewhat important, 0% Not important.
- Budgets: 24% Very important, 52% Important, 20% Somewhat important, 0% Not important.
- Investigative tools/solutions (including case management): 32% Very important, 45% Important, 19% Somewhat important, 0% Not important.
- Board level/senior management support: 30% Very important, 46% Important, 19% Somewhat important, 0% Not important.

Source: Chartis financial crime global survey
The EY point of view: Managing data throughout the customer life cycle

Effective financial crime risk controls are dependent on the data that is supplied to them – even the best control systems will be ineffective if the data provided is of poor quality. This is an issue that more and more organizations are identifying as a root cause to operational inefficiencies. There is a need for better data governance to be put in place, including data policies to define minimum standards and effective ongoing monitoring of these standards. In addition there is currently an increasing trend of organizations moving towards the use of a single data layer to supply data to all of their financial crime risk control systems, therefore ensuring a consistent set of data is used and reducing the number of feeds from source systems.

Looking at data management across the customer life cycle helps identify where financial crime risks are introduced, controls required to mitigate those risks, and ultimately what key data elements need to be captured for those controls to be effective (Figure 10).

Figure 6: The customer life cycle

Executing the integration process

The impetus for FIs to move toward integrated FCRM is readily apparent. The integration process that individual FIs follow, however, will vary in complexity and direction, depending upon multiple factors, such as size and organizational structure. Multi-national firms and those with multiple business lines will be facing particularly difficult challenges with respect to coordination and alignment across those business lines and borders.

Despite this, one commonality is that a phased approach will be required by all – such a transformation cannot be achieved overnight. Another common challenge for most FIs is that they will probably begin with roughly eight or nine main silos related to FCRM: AML, sanctions filtering, card fraud, ACH fraud, online fraud, employee fraud, trader surveillance, FATCA compliance and KYC, for example.

Given that the concept of simultaneously unifying all financial crime systems and processes under a single umbrella is unrealistic, FIs must identify the areas where there is least resistance to change in terms of their financial crime systems and processes under a single umbrella.

For most organizations, the alignment of fraud and AML systems and processes is a good place to start. As regulators become more restrictive in their approach, FIs are finding that they need to apply consistent investigation processes and controls to their fraud and AML assessments. Indeed, a number of FIs have already integrated their processes.
Decisions on data

As firms move toward integration, the success of the project will ultimately be determined by how effectively they can manage organizational data. We have outlined some of the different approaches and options that FIs may consider as they seek to integrate data management.

1. **Data integration**

To turn data into practical information, business intelligence systems need to manage the integration of metadata. This process has a number of steps, which are given below:

1. **Establishment** of the source to target data interface with extract and transformation logic conducted at the source.
2. **Intermediation** with a central data-staging layer to centralize transformation logic.
3. **Development** of messaging standards to allow sharing of information across networks and application-to-application connectivity.
4. **Introduction** of high performance infrastructure to speed up extraction of information and provide a central platform for fast search.
5. **Deployment** of data and analytics kernels to source platforms to pull data quickly through the enterprise, and speed up end-user decision-making.

Many FIs have reacted to the ever-increasing volumes of data they are required to process by investing in large data warehouse projects. These data warehouses are often cumbersome and slow, however, with lengthy and laborious extract, load and transform (ETL) processes.

We are seeing organizations adopt several different approaches to solve this problem. Some are moving to a “publish and subscribe” model, while others are converging regional standardized data hubs in an attempt to make data transfer faster and more efficient, while taking into account potential regional and cross-border data protection issues. Audits of data quality are also becoming increasingly common.

2. **Data alignment and abstraction**

One method for bringing data management systems together that does not involve breaking down silos is to use layered data abstraction processes that bridge across silos instead.

An abstraction layered data management architecture includes:

- **A base, physical layer** – where data sources are integrated, providing basic quality checks, type-casting, and name formatting.
- **A business layer** – where standardized methods of data description and modeling throughout the enterprise are applied to the metadata from the physical layer.
- **An application data layer** – where data is transformed into an accessible format for data consumers, whether these are customers or business users.

While the abstraction data layer system does not have the same speed and efficiency as an integrated data warehouse, the potential for quick implementation and therefore return on investment make it an attractive proposition, particularly for larger, complex organizations.

Managing the integration process

As with any business change process, it is important to create a structured roadmap at the outset that takes into account the organization’s current state, including any gaps, overlaps and efficiencies, and outlines the future state, such as shared capabilities, synergies and benefits.

Broad executive-level ownership and visible support for change will be important too, including leaders representing a cross-section of the organization committing time, resources and subject matter expertise.

Firms will also need to continue to run their existing systems in parallel with the creation of new, integrated systems in order to keep essential business processes running. For most large FIs, a change budget will be set aside, with a specific team set up to oversee the process, usually over a three- to five-year period. These teams will follow separate work streams, but their progress will be reviewed at group level to ensure their approach is aligned with the wider business. Careful construction of a roadmap for this process is critical, as the transformation process can and will change data sources behind applications and will affect their function. This balancing act of “run the bank” versus “change the bank” is a critical success factor.

Expenditure

It is obvious that the budget will strongly influence the approach that FIs are able to adopt as they move toward FCRM integration, in terms of how swiftly and how deeply the process goes.
Our survey results (Figure 7) reflect both the urgency of the issue and the potential of integrated FCRM to help reduce future costs, given that the majority of FIs intend to increase their expenditure on financial crime risk and compliance management technology, despite the current emphasis on cost cutting in the sector.

The greater part of the spending increase within the sector is likely to be tactical expenditure, focused on extending existing point solutions to conduct enhanced analytics, further compliance reporting, or buying new point solutions. At the same time, there is also likely to be a low volume of very high-value “change the bank” projects by tier 1 FIs, involving significant investment, and possibly the creation of financial intelligence units.

A financial crime reference architecture

A convergence trend in financial crime looks at common capabilities of reporting, case management, work flow, analytics and data across all financial crime risks to provide better information and intelligence sharing and drive efficiencies in risk management (Figure 8).
Conclusion

Today’s FIs are exposed to a wider range of risks than ever before, as they continually implement new technologies and open up new channels to customers in a bid to remain competitive. Meanwhile, regulators continue to pressurize firms to devote greater resources to assessing and reporting on financial crime and conduct risk.

Significant operational savings can be gained with centralized management of financial crime. The convergence of analytics, workflow and data management will increase transparency, increase agility and decrease duplication of effort when analyzing financial crime across business lines and international borders, creating complete views of customers across the entire transactional life cycle.

Those FIs that fail to face up to these risks and demands will be at a distinct disadvantage in future as customers, investors and shareholders all begin to attach greater value to the security and integrity of financial institutions, as well as reputation and brand protection.

What will be needed, therefore, is an integrated approach to the management of financial crime risk and compliance that will help them to better detect criminal attacks and fraud and avoid regulatory fines, and ultimately reduce their costs as a result of operational efficiency savings and tighter security.
About the EY contributors

Patrick Craig
EMEIA Compliance IT Advisory Leader

Patrick has been with EY for more than six years and runs the EMEIA Compliance IT Advisory practice. This practice provides IT strategy, transformation, optimization and analytics services on monitoring, surveillance, investigation and reporting platforms to global financial services institutions to help manage risk. Prior to this role, he was responsible for building EY’s compliance IT advisory capability in New York. Previous to working at EY Patrick was head of services for Searchspace, an AML technology company that is now part of the Nice Actimize corporation. Patrick gives lectures at the International Compliance Association on the topic of compliance technology and speaks at international conferences on AML and financial crime trends.

Renato V. Giammarco
Americas Compliance IT Advisory Leader

Ron has been with EY for more than 20 years and runs the Americas Financial Services Compliance IT Advisory practice and is part of EY’s Americas IT Advisory Leadership team. This practice provides IT strategy, transformation, implementation optimization and analytics services on governance, monitoring, surveillance, investigation and reporting platforms to global financial services institutions to help manage regulatory requirements and financial crime related risks. Ron is a frequent speaker at industry conferences and roundtables and has been a guest lecturer at universities and colleges on the topics of anti-money laundering, consumer financial protection and fraud prevention.

Scott Samme
EMEIA Compliance IT Advisory Director

Scott has been advising and delivering technology solutions related to financial crime prevention for more than nine years. He has experience across different industries, including banking, insurance, national intelligence and policing, addressing Fraud, AML, Sanctions, organized crime and intelligence in different geographies. Previous to working at EY, Scott was the head of services globally for BAE Detica NetReveal.
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 global user conference for 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

Visit www.chartis-research.com for more information.
Further Chartis reading

- RiskTech100 2015

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