Market Quadrants

Cyber Risk Quantification Solutions, 2020

Market Update and Vendor Landscape

Chartis

Independent. Insightful. Actionable.

About Chartis

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

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

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

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

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

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

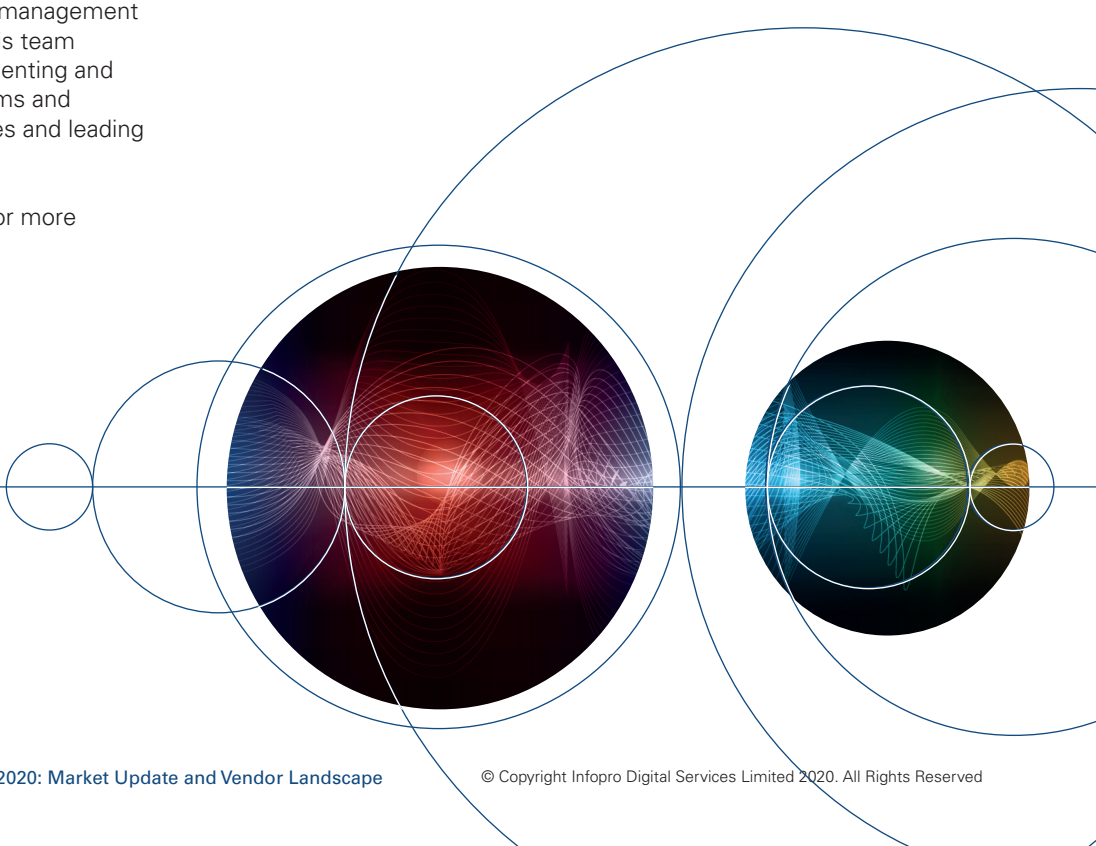


Table of contents

1. Executive summary 5

2. Market update 7

3. Vendor landscape 11

4. Appendix A: Glossary 15

5. Appendix B: RiskTech Quadrant® methodology 17

6. How to use research and services from Chartis 21

7. Further reading 22

List of figures and tables

Figure 1: RiskTech Quadrant® for cyber risk quantification solutions, 2020 13

Figure 2: Example Monte Carlo simulation 15

Figure 3: Example probabilistic model 15

Figure 4: Example random forest 16

Figure 5: RiskTech Quadrant® research process 17

Figure 6: RiskTech Quadrant® 18

Table 1: Assessment criteria for vendors of cyber risk quantification solutions, 2020 14

Table 2: Vendor capabilities for cyber risk quantification solutions, 2020 14

1. Executive summary

As cyber risk quantification (CRQ) technology matures, and as CRQ solutions make more use of advanced analytics (including artificial intelligence [AI]), we are seeing a divergence in the market. Encouraged by the prospect of easier sales, CRQ solution vendors are targeting corporates rather than financial services companies. And as the number of vendors offering CRQ solutions grows, CRQ offerings themselves are diversifying into two main approaches we can define as follows:

- **'Governance, risk management and compliance (GRC) for cyber'** offerings. These provide quantification and modeling tools focusing on compliance and governance, to help firms comply with regulations, external cybersecurity standards and internal risk appetites. They also help firms create or navigate cybersecurity frameworks, with an emphasis on easy-to-use software and well-developed visualizations. Uptake has been higher among corporates and non-financial institutions (FIs).

- **'Statistically driven CRQ'** offerings. These are rating, risk-scoring and risk-attribution-related models, which decompose the total risk of a portfolio into smaller terms. This approach is more numerically driven, providing detailed statistical analysis behind cyber-risk scores. It usually involves an analysis of the probability and/or impact of a potential cyber breach. These offerings have the advantage of being the foundation of both quantitive risk and analytics approaches (including IT asset portfolio management, capital at risk models, risk attribution and risk allocation), and quantitive control and governance frameworks.

Larger banks tend to build their cyber-risk analysis systems in-house and rely on insurers to cover their cyber risk. Because of their hierarchical structure and large compliance teams, bigger banks also tend to have advanced analytics tailored to their requirements. Insurers, which have data on the losses that can be incurred after breaches, are best positioned to fill any data gaps, and can provide financial coverage if breaches do occur.

CRQ in financial services: opportunities and challenges

The main opportunity within financial services is to sell CRQ solutions to small and medium-sized banks, for the reasons outlined above. These institutions could benefit from a blend of offerings, to support their cyber-risk governance and help them prioritize tasks to improve their cybersecurity. This is useful for two reasons:

- By doing so they can significantly reduce their cyber risk, and possibly protect their systems from a breach.

- They can position themselves as one step ahead of regulators, saving themselves time and cost if they have to comply in the near future.

However, for this to succeed a major structural challenge must be addressed: the communications gap between FIs (and their CROs) and technology vendors. FIs can find it hard to understand the technological nature of cyber risk, while vendors can struggle to comprehend and articulate what FIs actually need (especially in providing transparency and clarity around modeling methodologies).

Among those entities that can help to bridge this gap are regulators and central banks. The latter group in particular is well-positioned to take a broad view of existing CRQ offerings and identify exactly what FIs need. Chartis expects that central banks will soon require FIs to report on how they measure their cyber risk, further enhancing their knowledge of the subject and, by extension, boosting demand for CRQ solutions among banks themselves.

Equally, vendors that can communicate and distrubute their methodologies and frameworks in the context of an evolving regulatory landscape will have an advantage.

An evolving vendor landscape

The vendor landscape for CRQ solutions is also evolving: the range of CRQ methods being used is expanding significantly, and these methods are maturing technologically. In addition, driven partly by demand among corporates, vendors have made major developments to their visualization capabilities.

As highlighted above, among the range of available CRQ solutions, two competing models have emerged. The first one, 'GRC for cyber' is more qualitative in nature, relying largely on expert opinion supported by statistics. The second – the 'statistically driven CRQ' model – relies more on data and statistical analysis. Both involve

quantification to some extent, and – as we explore in more detail – both have their strengths and weaknesses.

This report uses Chartis' RiskTech Quadrant® to explain the structure of the market. 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 risk-management solution; rather, it has a sophisticated ranking methodology to explain which solutions would be best for buyers, depending on their implementation strategies.

This report covers the following providers of CRQ solutions: Balbix, BitSight, CounterCraft, CYR3CON, eFortresses, FICO, foreseeti, FortifyData, Maxxsure, RiskRecon, RiskSense and SecurityScorecard.

We aim to provide as comprehensive a view of the vendor landscape as possible within the context of our research. Note, however, that not all vendors we approached provided adequate information for our analysis, and some declined to participate in our research[1].

[1] *Note that mention of any vendor in the text of this report does not constitute an endorsement of its products by Chartis.*

2. Market update

Changes in the CRQ landscape since our last report[2]

CRQ may be a relatively small part of the market for cyber risk management solutions, but it is growing rapidly. This is partly because all FIs – large and small alike – must increasingly accomplish several goals:

- Understand the cyber-risk profile of their organizations.
- Understand, analyze, allocate and define their cyber-risk management frameworks.
- Comply with external standards.

To define or model its cyber-risk portfolio, every company needs some form of analytical and quantification framework.

Key trends

The key market trend we have observed in our latest research is the ongoing diversification of the landscape into two approaches:

- **'GRC for cyber'**. Quantification and modeling that focus on compliance and governance, to help FIs understand cyber risk and create or navigate their cybersecurity frameworks, with an emphasis on easy-to-use software and more sophisticated visualizations. While a broad range of models, methodologies and outputs exists, the general approach is to focus on providing overarching governance, control and compliance frameworks. Some vendors focus on developing internal compliance and control capabilities (defining risk posture[3], visualizing enterprise or business-unit risks, or helping to define control frameworks), while others focus on enabling compliance with regulatory and industry standards (such as the Health Insurance Portability and Accountability Act [HIPAA] and General Data Protection Regulation [GDPR]). Many vendors offer a blend of the two. The approach often follows the Factor Analysis of Information Risk (FAIR) standard.
- **'Statistically driven CRQ'**. In contrast, statistically driven CRQ frameworks focus on generating event probabilities, using rating, risk-scoring and risk-attribution-related models. These approaches are more quantitative, providing detailed statistical analysis behind cyber-risk scores, and they often involve an analysis of the probability and/or impact of a potential cyber breach. They can also be leveraged to build fully fledged statistically and analytically robust risk, portfolio management, attribution, control and governance frameworks. These methods leverage the sheer volume of data available both internally and externally – as ongoing digitalization increases the availability of detailed data on the state of FIs' internal networks and operating business environments. Finally, each quantification methodology is slightly different, depending on the data and models used in the analysis.

Since we last analyzed the market, sales of solutions in the first category have increased rapidly, driven by demand from corporates rather than FIs. Companies in many industries (such as retail and manufacturing) are being exposed to increasing levels of cyber threat, and their demand for holistic solutions – such as those provided by CRQ systems – is growing rapidly in tandem.

Corporates demand different things from vendors: they tend to focus on solutions that are easy to use, with more sophisticated visualization capabilities, and which improve users' general understanding of the market. Equally, they don't need as detailed an understanding of the underlying methodology, so require lower methodological transpaerency.

In addition, the level of statistical sophistication and rigor in the corporate environment can differ considerably from that in FIs. In non-financial services companies, data and methodology are useful and important, but visualization – the ability to manipulate data quickly and conveniently – is more useful. In the financial industry, firms focus more on the breadth and level of detail of numerical data.

In financial services, sales of CRQ software are still highest in the insurance sector, and this remains the main stimulus for developing CRQ solutions in the industry. As we commented in our previous CRQ report, insurance brokers and underwriters both benefit from quantifying their cyber risk. Brokers use CRQ mainly to inform decisions and advice around policy selection and risk-reduction,

[2] *'Cyber Risk Quantification Solutions, 2019: Market and Vendor Landscape'.*
[3] *'Risk posture' in this context refers to the status of a firm's cybersecurity infrastructure: the strength of its cybersecurity policies and how effectively they mitigate risk.*

while underwriters use it mainly for policy pricing and portfolio optimization[4].

Although banks are adopting CRQ solutions, uptake remains slow. FIs are often unsure about how to align CRQ models with their internal risk models and asset-acquisition policies. Larger banks tend to rely on insurance companies to cover them in case of a breach, and have internal solutions that give them an acceptable level of protection from cyber risk[5]. Nevertheless, while there is currently no regulation in place that requires FIs to measure their cyber risk, regulators' heightened focus on IT resilience may yet increase banks' appetite for CRQ solutions.

The CRQ challenge in financial services: external vs. internal solutions

The first, more GRC-oriented, CRQ solutions were based on quantification and modeling systems that focused on compliance and governance. Because big banks can create these in-house, their demand for these types of solutions is low.

Demand in the market for the second, more statistically focused type of solution, which is based on rating, scoring and risk-attribution-related models, depends on vendors' ability to provide:

- Data at scale. The ability to analyze very large data sets that can be acquired using scalable and largely automated processes.
- Cross-institution and cross-industry comparisons.
- The technical and statistical depth to map an FI's entire attack surface and address the cyber challenges it may face.

Compared to corporates, FIs also focus more on cyber risks in their *internal* infrastructure – not just those that originate from *outside* the organization. FIs also have complex legal and operating structures. As a result, demand for features that analyze the hierarchies, structures and counterparties within their organizations is stronger, and enabling the proper organizational allocation of risks is critical.

Some technology vendors claim that they can switch from an external focus to an internal one if required. Internal networks require a different methodology, however, which can take time to develop. Within the financial services industry, CRQ vendors that tend to approach the issue from an external perspective already meet the demand coming from insurance companies. Insurers use CRQ data as a reference point to help them improve their own methodologies, as input data into their in-house analytics, or to challenge managers that believe they have robust cybersecurity.

Insurers have the advantage of having actual loss data, and provide cyber-risk solutions themselves. Banks, on the other hand, are direct consumers of data (they need to leverage it to determine the security of their own networks and the fair value of insurance required), but they also need data to judge which counterparties and vendors their networks should be exposed to. In many ways the growth of CRQ in third-party risk analysis is conceptually simpler than leveraging CRQ systems for internal risk models (which implies alignment and integration of CRQ vendors' methodology with internal risk frameworks).

The CRQ opportunity in financial services

For larger banks, implementing many of the available CRQ solutions may not be the most efficient use of time and resources. They have a fairly clear understanding of their infrastructure and what protection they need, and without the commensurate availability of highly transparent and clearly communicated frameworks, or powerful regulatory frameworks, they have no real incentive to make major structural shifts.

Small and medium-sized banks, however, could benefit by cooperating with vendors, using a blend of CRQ vendors and solutions to help them manage their technology portfolios. Senior executives will require them to build tools to help manage their internal IT infrastructure. This process can be accelerated by acquiring CRQ tools – especially those with a more GRC focus – and more quantitative, statistically oriented ones that they can't build in-house.

CRQ solutions can also help smaller and medium-sized banks match larger institutions in terms of their cybersecurity and protection against breaches, by outsourcing the task to CRQ vendors. The smaller the bank, the more important external CRQ solutions become (whatever the level of externalization). This can help the firm address challenges in building a quantitative infrastructure,

[4] *For more information, see* page 6 of the Chartis report '*Cyber Risk Quantification Solutions, 2019: Market and Vendor Landscape'.*
[5] *The original CRQ solutions, such as those based on the* FAIR *model, were governance-oriented, and were not designed for banks.*

Central banks and CRQ

While it is unclear how far central banks understand the cyber risk landscape, their desire to understand CRQ technology has been increasing for some time, accelerated in recent months by the COVID-19 pandemic. Because of the crisis, many companies have moved their operations out of offices to form distributed network structures in which employees work from home or remote locations. Because this activity increases FIs' cyber risk, interest in cyber-risk solutions among banks is growing – and we expect it to increase further within the next few months, when there is more scope and time to take stock and re-plan after the initial upset.

Although CRQ is technologically advanced, central banks are well placed to bridge the communications gap between technology vendors and FIs. There is currently a growing belief in the market that cyber risk is systemic* (systemic risk is the risk of an entire market or system failing), and that central banks are well-equipped to reduce systemic risks. The European Systemic Risk Board (ESRB), for example, has already developed an analytical framework to assess how cyber risk can become a source of systemic risk to the financial system†.

** In a survey of a global group of experts by insurance firm AIG, more than 90% of respondents believed that cyber risk is systemic. About 60% felt there was a 50% or greater chance of an event affecting multiple companies in the subsequent 12 months, while more than half felt there was a 10% or greater chance of an event impacting 50 to 100 companies (see* **https://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/aig-cyber-risk-systemic-final.pdf** *and* **http://web.stanford.edu/~csimoiu/doc/Global_CRQ_Network_Report.pdf***).*

† **https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf**

a cyber policy, or a technology portfolio management and control process[6].

Communication must improve

First, however, communication about CRQ between vendors and FIs must improve. Vendors can find it difficult to explain their offerings to banks: coming largely from a technology-based environment they may be less knowledgeable about portfolio management or incremental risk. They tend not to use statistics when explaining their offerings – a crucial requirement for FIs – and they rarely describe them in quantitative terms.

For their part, CROs can struggle to understand cyber risk, despite frequent questioning about it from management and the wider business. Chartis believes that for many CROs, cyber risk so far has been a largely qualitative concept. This is emphasized by vendor frameworks, models and structures that have neither provided sufficient transparency nor aligned with existing risk frameworks – although this is improving, and a few leading vendors are beginning to explore further. The qualitative focus is especially true for compliance- and governance-focused solutions, which rely on abstract concepts (such as risk posture) that are difficult to entirely reconfigure in quantitative terms.

Even when cyber risk is more quantitative, ratings models are often not explained in detail – where a number comes from, for example, how it is calculated, or why it was calculated in a particular way. Instead the explanations rely heavily on IT terminology unfamiliar to CROs.

Ultimately, however, CROs need to apply a numerical and quantitative framework with methodological and statistical transparency to a problem. Sometimes a challenge emerges because of the machine learning (ML) and neural-network-based models the vendors are leveraging.

But because vendors do not know how to explain their offerings to financial services companies, and financial firms do not know how to assess vendors' solutions, we are seeing a communications gap emerging between the CRO community and CRQ technology vendors. A third party to bridge the gap is vital – a role that could be filled well by central banks or regulators.

Looking ahead…

Looking ahead, we expect three main trends in the CRQ market:

- Cyber-risk insurance will continue to be the main driver behind the development of CRQ solutions.
- Use among corporates will continue to grow.

[6] *This also extends to the corporate sector: large companies can have holistic cyber-defence software systems, while smaller firms do not, and may need a managed CRQ service.*

- Intervention from regulators/supervisors will affect demand for CRQ solutions.

Insurance firms are considering offering CRQ solutions to their clients, rather than using them predominantly as a reference point. For many insurance providers, assessing the cyber risk of small and medium-sized companies with little publicly available information can be a challenge, so CRQ solutions could assist them in that area. And by offering CRQ tools, insurance firms could go beyond helping their clients assess their cyber risk to helping them control and reduce it.

Most **corporates**, meanwhile, are likely to be required to comply with a range of standards related to cyber risk, and many existing regulatory standards will incorporate some element of cyber risk. Firms will be looking to leverage CRQ in their supply-chain frameworks (to assess third-party risk, for example), and corporates will increasingly be required to make more disclosures about their risks – including cyber risk. To disclose the potential risks they will need to understand and apply quantitative and rating methods.

The regulation trigger

In the wider financial services industry, Chartis believes that FIs' demand for CRQ solutions will be triggered by action from a regulator or central bank. Regulators' interest in cyber risk is already growing. In some jurisdictions in regions and countries such as Hong Kong, Singapore, the UK and the US, specific regulatory initiatives already exist around banks' cyber risk, and FIs are expected to identify critical information assets that they must protect. One common requirement is for banks to test their vulnerability and resilience to cyber risk (using penetration testing, for example), and to report cyber breaches. Another is for banks to have clear responsibilities and accountabilities in their systems, to help protect them from breaches[7].

Supervisors' approaches are also evolving, becoming more tailored to assessing banks' cyber risk. The International Monetary Fund (IMF) has called on all supervisory agencies to 'quickly establish a framework for cybersecurity risk supervision'[8]. And the Bank of International Settlements has published a paper in which it offers high-level policy considerations for banking supervisory authorities planning to introduce or develop their tools[9].

We expect that, as a next step, regulators will require banks to report on how they measure cyber risk. In the UK, the Financial Conduct Authority (FCA), the Bank of England (BoE) and the Prudential Regulation Authority (PRA) recently published a joint Consultation Paper on Operational Resilience that also covers cyber attacks[10]. In its consultations this year, the BoE is already asking FIs about their IT resilience, forcing firms to reach a better understanding of their environment. We expect that it will also start to ask banks about how they understand, measure and quantify their cyber risk.

Historically, the BoE has proved it is less concerned about a lack of full clarity around the subject, and has expressed a willingness to enter the space as a regulator. Thus it will likely be the first central bank to introduce policies that require FIs to report how they measure cyber risk. As a result of its consultations, the BoE is likely to understand the problem well enough to introduce new measures soon. Any measures it does introduce will likely be principles-based, allowing it to examine the tools that FIs have and educate itself on current market practices.

[7] **https://www.bis.org/fsi/publ/insights2.pdf**
[8] *'Cybersecurity Risk Supervision', Christopher Wilson, Tamas Gaidosch, Frank Adelmann and Anastasiia Morozova; IMF (Monetary and Capital Markets Department), 2019.*
[9] **https://www.bis.org/fsi/publ/insights2.pdf**
[10] **https://www.fca.org.uk/news/speeches/view-regulator-operational-resilience**

3. Vendor landscape

Overview

CRQ is evolving – more methods are being used, and they are becoming more technologically advanced. Vendors have started to employ methods such as Monte Carlo simulations to predict cyber breaches, for example, as well as probabilistic graphical models and random forests[11].

Vendors are also employing ML more often in their solutions – although it can sometimes be used to mask the lack of a robust methodology behind a particular quantification technique. Because the data used for CRQ is usually non-linear and can be highly dimensional and voluminous, it lends itself well to ML and non-linear models. In evaluating the effectiveness of an ML model, however, it's vital to consider how the data is organized and fed into it.

Vendors have also made extensive developments to visualization capabilities, driven partly by the demand from corporates. Corporates tend to prefer visual analysis over text or numerical analysis, because it is easier to understand and takes less time to communicate. And in contrast to FIs, corporates have less need to accompany their analysis and visualizations with a statistical methodology.

The divergence in CRQ models and solutions

As highlighted in the market update section, among the range of available CRQ solutions, two competing models have emerged. The first one, 'GRC for cyber' is more qualitative in nature (particularly in its presentation and operationalization). The second – the 'statistically driven CRQ' model – provides more foundational statistical and quantitative outputs, such as ratings and event probabilities. Both involve quantification to some extent, and both have their strengths and weaknesses.

GRC for cyber

Vendors of 'GRC for cyber' solutions often tend to focus on process, steered by regulatory compliance, with the aim of helping companies understand how well their processes are functioning.

The problem with this approach, however, is that many CROs in banks find it hard to work with. The underlying data is statistically intractable and may or may not correspond with what has happened or what will happen, creating an operational challenge.

Statistically driven CRQ

This approach is based on analyzing large amounts of data. It has been made possible only recently thanks to a vast increase in the amount of available data. Quantification has traditionally been a challenge because of the small number of total cyber incidents and a lack of publicly available data. In the past few years, however, some vendors have started to collect data from the internet and companies' IP addresses. As companies digitalize and move online, they reveal a great deal of information about the state of their IT infrastructure.

Those vendors able to take daily 'snapshots' of the internet – perhaps as many as a few million IP addresses every day (or as many as a vendor deems relevant) – could embark on historical analysis of statistical data. Simply by examining this data, vendors may notice that companies have ports that are open or web servers that are outdated. Vendors that decide to base their solutions on this approach have started to gain a sense of firms' 'hygiene profiles'. And following the explosion of data in recent years, vendors have been able to take a truly statistical approach to cyber risk.

Nevertheless, while this model works well for companies with large amounts of available data, it is tailored more to institutions that are already more aware of their cyber risk and able to mitigate it, and which are looking for software to help them identify and fix weak points. For companies facing major IT restructuring projects, the 'GRC for cyber' approach is likely to be a better initial fit, because it can help them build a cybersecurity skeleton that complies with regulations and is up to date with expert industry analysis.

Vendor types

As well as differentiating vendors according to the two approaches considered above, we can also divide them into those that are *internally* or

[11] *For more information on these techniques, see Appendix A: Glossary.*

externally oriented. Vendors that quantify cyber risk from an *internal* perspective use either a firm's internal historical loss data, as well as information on the frequency of breaches, or apply a simulation engine to a representational mapping of the firm's internal network. Vendors that produce risk scores using the *external* methodology rely on internet-scale data collection, gathering information on all internet-connected networks at their boundaries[12].

Chartis RiskTech Quadrant® and vendor capabilities for CRQ solutions, 2020

Quadrant commentary

As CRQ technology evolves, so does the vendor landscape. The number of vendors has grown – crucially, our quadrant represents only a small sample of the vendors currently in the market[13]. This is largely because many vendors have moved to the corporate side, where it is easier to sell, having decided they no longer want to wait for growth in demand among FIs.

As a result, vendors tend to cluster based on their capabilities. Even within clusters companies can operate in different markets – several sub-markets exist within the overall CRQ space, largely aligned with different sectors of the economy. In addition, 'GRC for cyber' and 'statistically driven CRQ' technology offerings each have distinct markets.

While *best-of-breed* vendors have a relatively narrow completeness of offering, their solutions vary significantly, and while they have similar market potential, they can target different markets. The main differentiating factor for their solutions is shaped by the CRQ model they choose. We expect them to grow quickly, supported predominantly by corporate clients.

Point-solution vendors target particular niches in the market, and their offerings can differ significantly. Vendors in this quadrant include companies that focus on internally oriented data points, as well as 'GRC for cyber' vendors. As they grow, however, these companies and best-of-breed firms may diverge into different markets.

The lack of *enterprise solutions* in our quadrant emphasizes the current state of the CRQ market.

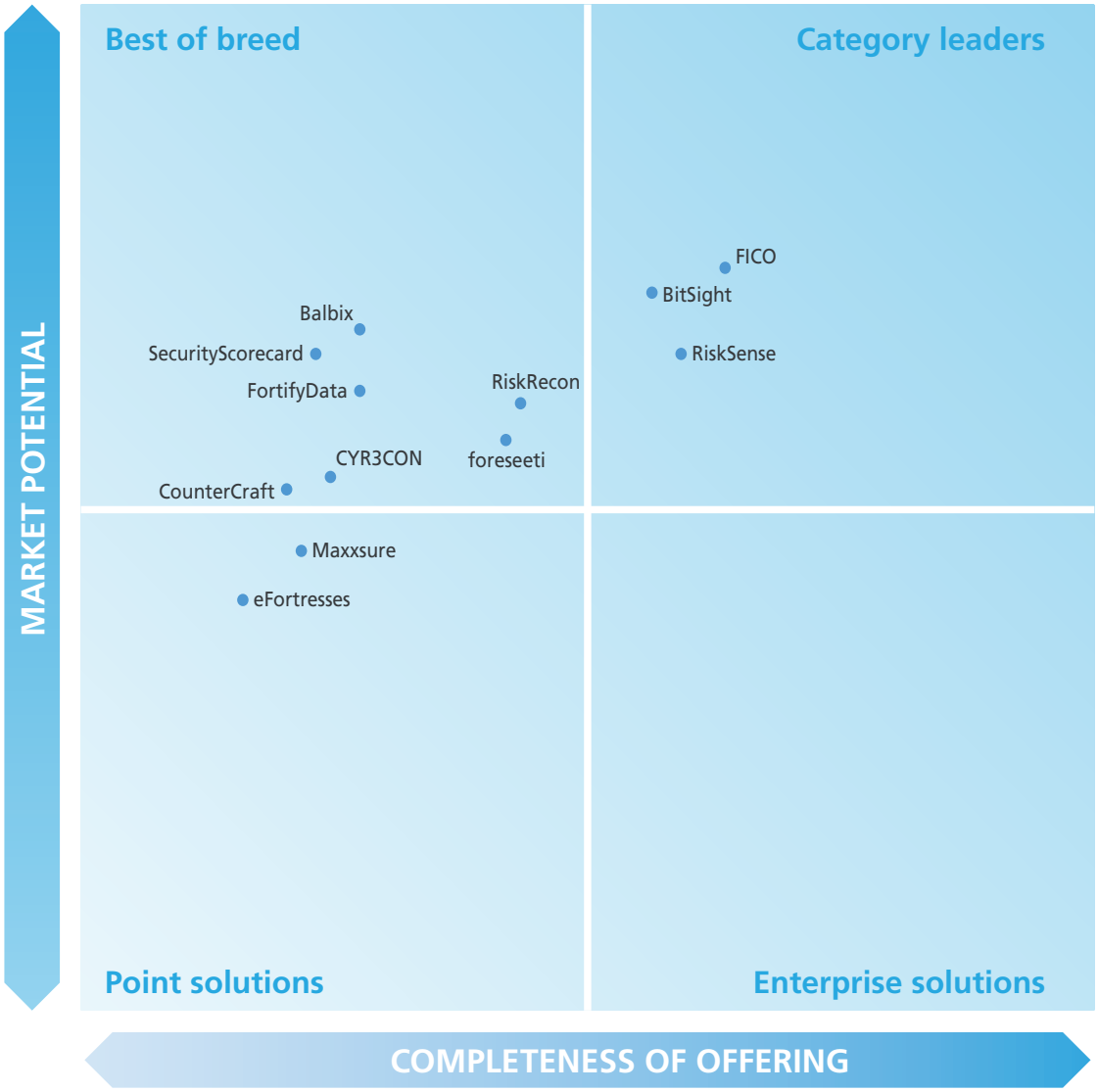
In terms of completeness of offering and market potential, *category leaders* form a relatively close cluster. Similarly to best-of-breed vendors, however, they target different companies, so in some instances may not regard each other as competitors.

Looking ahead, we expect the market to evolve rapidly, as vendors develop broader solutions, gain clients and move into other cyber-risk-management markets (such as threat intelligence). Most vendors currently have clients across industries, but this may change as they start to specialize and focus on meeting the needs of one or two specific client types.

Figure 1 illustrates Chartis' view of the vendor landscape for CRQ solutions. Table 1 lists the completeness of offering and market potential criteria we used to assess the vendors. Table 2 lists the vendor capabilities in this area.

[12] *For more information, see pages 10 and 11 of the Chartis report 'Cyber Risk Quantification Solutions, 2019: Market and Vendor Landscape'.*
[13] *Our focus has been on vendors for which we believe we have sufficient data to make an effective determination of their position.*

Figure 1: RiskTech Quadrant® for cyber risk quantification solutions, 2020



Source: Chartis Research

Table 1: Assessment criteria for vendors of cyber risk quantification solutions, 2020

Completeness of offering	Market potential
• Internal/inside-out risk scoring	• Customer satisfaction
• External/outside-in risk scoring	• Market penetration
• Loss estimation	• Growth strategy
• Portfolio optimization and simulation	• Financials
• Workflow and integration	• Business model

Source: Chartis Research

Table 2: Vendor capabilities for cyber risk quantification solutions, 2020

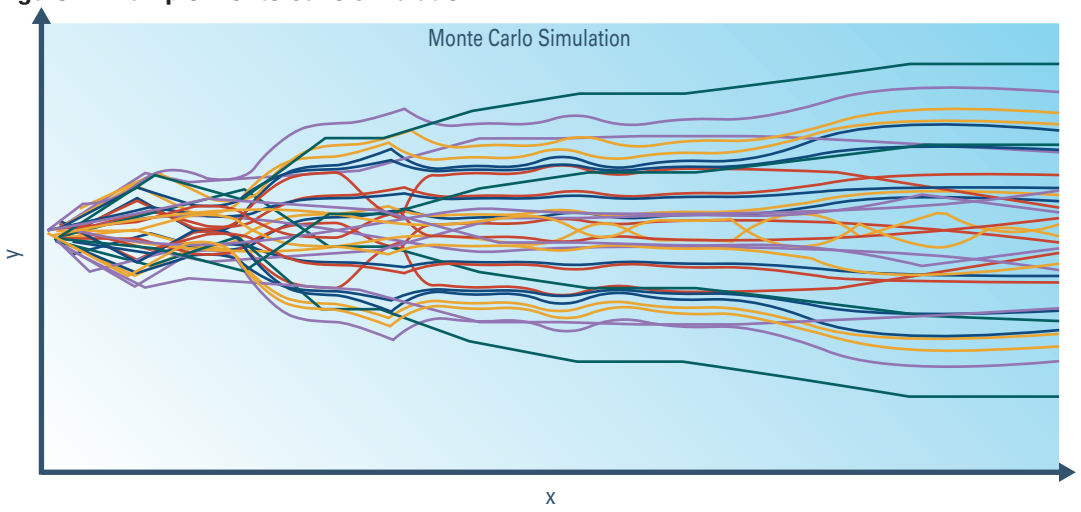
Vendor	Internal/ inside-out risk scoring	External/ outside-in risk scoring	Loss estimation	Portfolio optimization and simulation	Workflow and integration
Balbix	**	**	*	**	**
BitSight	***	***	***	***	**
CounterCraft	**	**	*	**	**
CYR3CON	**	**	*	**	**
eFortresses	***	*	*	*	**
FICO	***	****	***	***	***
foreseeti	**	**	**	**	**
FortifyData	***	***	*	*	**
Maxxsure	**	*	*	**	**
RiskRecon	**	**	**	**	**
RiskSense	***	***	***	***	**
SecurityScorecard	**	**	**	*	**

*Key: **** = Best-in-class capabilities; *** = Advanced capabilities; ** = Meets industry requirements; * = Partial coverage/component capability*
Source: Chartis Research

4. Appendix A: Glossary

Monte Carlo simulation. A computational technique used in scientific applications to model outcomes according to a process driven by uncertain factors[14] (see Figure 2).

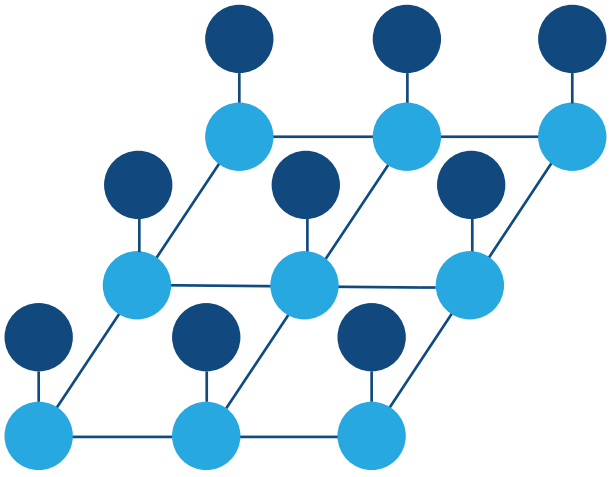
Figure 2: Example Monte Carlo simulation



Source: Chartis Research

Probabilistic graphical models. Probabilistic models for which graphs express the conditional dependence structure between random variables, helping analysts to understand how variables influence each other in a causal manner[15] (see Figure 3).

Figure 3: Example probabilistic model

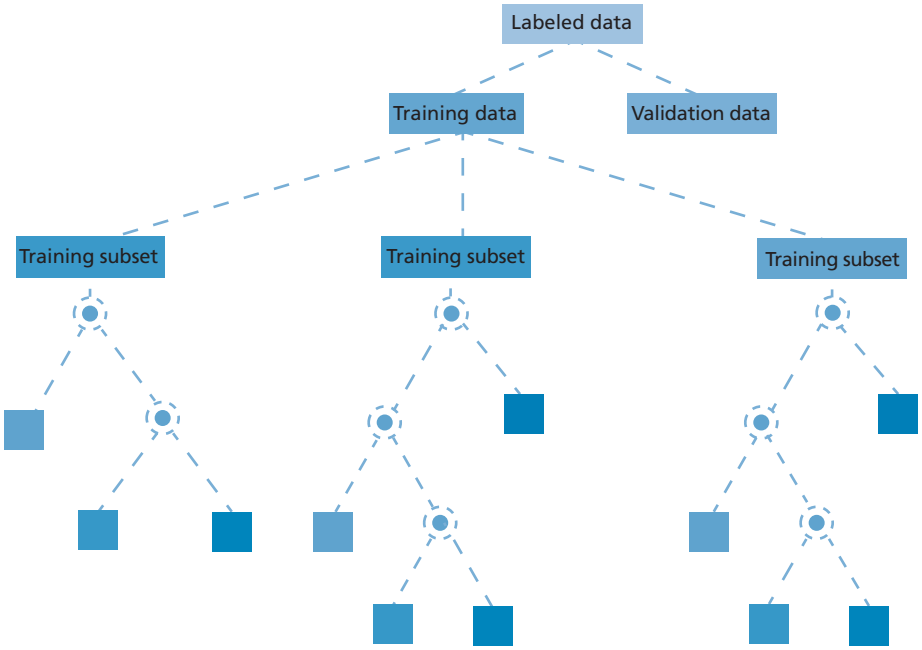


Source: Chartis Research

[14] *Definition from* **https://www.risk.net/definition/monte-carlo-simulation**
[15] *Definition from* **https://www.risk.net/risk-management/2426700/probabilistic-graphical-models-a-new-way-of-thinking-in-financial-modelling**

Random forests. Random forests work by trying various combinations of variables from all the data provided, to build an extended family of 'decision trees'[16] (see Figure 4).

Figure 4: Example random forest



Source: Chartis Research

[16] *Definition from* **https://www.waterstechnology.com/technology/4321656/not-random-and-not-a-forest-black-box-ml-turns-white**

5. Appendix B: RiskTech Quadrant® methodology

Chartis is a research and advisory firm that provides technology and business advice to the global risk management industry. Chartis provides independent market intelligence regarding market dynamics, regulatory trends, technology trends, best practices, competitive landscapes, market sizes, expenditure priorities, and mergers and acquisitions. Chartis' 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' 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' opinion. Risk technology vendors cannot purchase or influence positive exposure. Chartis adheres to the highest standards of governance, independence, and ethics.

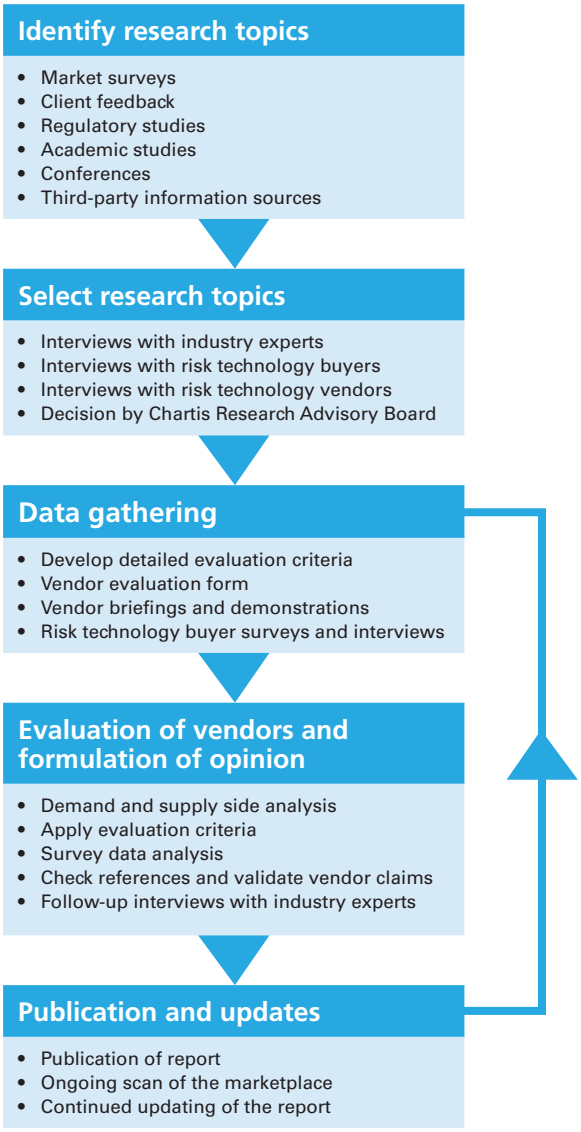
Inclusion in the RiskTech Quadrant®

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

Research process

The findings and analyses in the RiskTech Quadrant® reports reflect our analysts' considered opinions, along with research into market trends, participants, expenditure patterns, and best practices. The research lifecycle usually takes several months, and the analysis is validated through several phases of independent verification. Figure 5 below describes the research process.

Figure 5: RiskTech Quadrant® research process



Source: Chartis Research

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

- **Chartis vendor evaluation forms.** A detailed set of questions covering functional and non-functional aspects of vendor solutions, as well as organizational and market factors. Chartis' vendor evaluation forms are based on practitioner level expertise and input from real-life risk technology projects, implementations, and requirements analysis.
- **Risk technology user surveys.** As part of its ongoing research cycle, Chartis systematically surveys risk technology users and buyers, eliciting feedback on various risk technology vendors, satisfaction levels, and preferences.
- **Interviews with subject matter experts.** Once a research domain has been selected, Chartis undertakes comprehensive interviews and briefing sessions with leading industry experts, academics, and consultants on the specific domain to provide deep insight into market trends, vendor solutions, and evaluation criteria.
- **Customer reference checks.** These are telephone and/or email checks with named customers of selected vendors to validate strengths and weaknesses, and to assess post-sales satisfaction levels.
- **Vendor briefing sessions.** These are face-to-face and/or web-based briefings and product demonstrations by risk technology vendors. During these sessions, Chartis experts ask in-depth, challenging questions to establish the real strengths and weaknesses of each vendor.
- **Other third-party sources.** In addition to the above, Chartis uses other third-party sources of information such as conferences, academic and regulatory studies, and collaboration with leading consulting firms and industry associations.

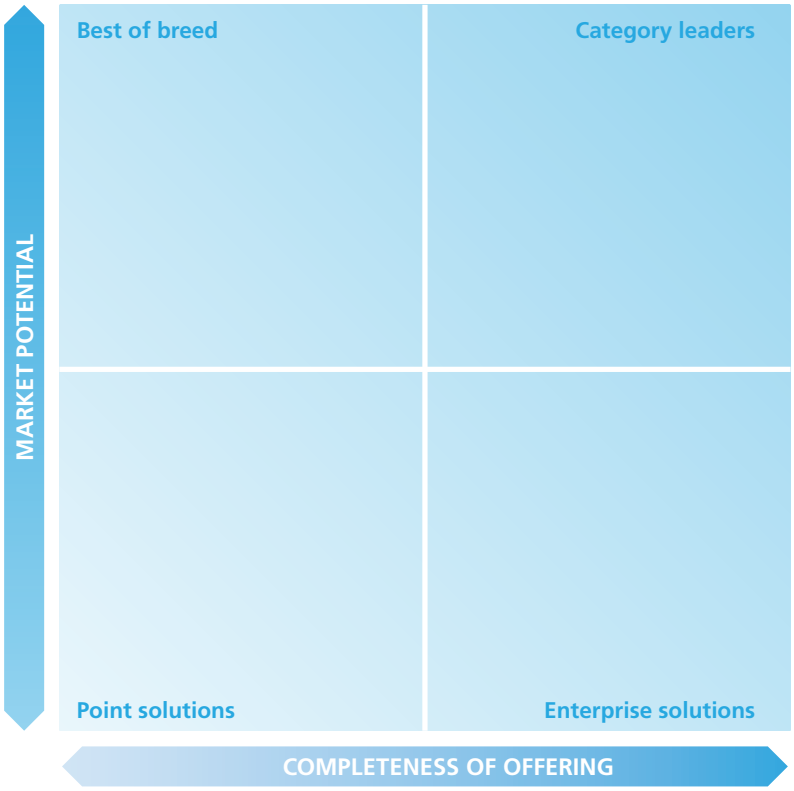
Evaluation criteria

The RiskTech Quadrant® (see Figure 6) evaluates vendors on two key dimensions:

1. Completeness of offering

2. Market potential

Figure 6: RiskTech Quadrant®



Source: Chartis Research

We develop specific evaluation criteria for each piece of quadrant research from a broad range of overarching criteria, outlined below. By using domain-specific criteria relevant to each individual risk, we can ensure transparency in our methodology, and allow 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

- **Business model**. Includes implementation and support and innovation (product, business model and organizational). 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. Also evaluated are new ideas, functionality and technologies to solve specific risk management problems. Speed to market, positioning, and translation into incremental revenues are also important success factors in launching new products.

- **Market penetration**. Volume (i.e. number of customers) and value (i.e. average deal size) are considered important. Rates of growth relative to sector growth rates are also evaluated. Also covers brand awareness, reputation, and the ability to leverage current market position to expand horizontally (with new offerings) or vertically (into new sectors).

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

- **Customer satisfaction**. Feedback from customers is evaluated, 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).

- **Growth strategy**. Recent performance is evaluated, including financial performance, new product releases, quantity and quality of contract wins, and market expansion moves. Also considered are the size and quality of the sales force, sales distribution channels, global presence, focus on risk management, messaging, and positioning. Finally, business insight and understanding, new thinking, formulation and execution of best practices, and intellectual rigor are considered important.

Quadrant descriptions

Point solutions

- Point solutions providers focus on a small number of component technology capabilities, meeting a critical need in the risk technology market by solving specific risk management problems with domain-specific software applications and technologies.
- They are often strong engines for innovation, as their deep focus on a relatively narrow area generates thought leadership and intellectual capital.
- By growing their enterprise functionality and utilizing integrated data management, analytics and BI capabilities, vendors in the point solutions category can expand their completeness of offering, market potential and market share.

Best-of-breed

- Best-of-breed providers have best-in-class point solutions and the ability to capture significant market share in their chosen markets.
- They are often distinguished by a growing client base, superior sales and marketing execution, and a clear strategy for sustainable, profitable growth. High performers also have a demonstrable track record of R&D investment, together with specific product or 'go-to-market' capabilities needed to deliver a competitive advantage.
- Focused functionality will often see best-of-breed providers packaged together as part of a comprehensive enterprise risk technology architecture, co-existing with other solutions.

Enterprise solutions

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

Category leaders

- Category leaders combine depth and breadth of functionality, technology and content with the required organizational characteristics to capture significant share in their market.
- Category leaders demonstrate a clear strategy for sustainable, profitable growth, matched with best-in-class solutions and the range and diversity of offerings, sector coverage and financial strength to absorb demand volatility in specific industry sectors or geographic regions.
- Category leaders will typically benefit from strong brand awareness, global reach and strong alliance strategies with leading consulting firms and systems integrators.

6. How to use research and services from Chartis

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

For risk technology buyers

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

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

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

Our vendor selection services include:

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

For risk technology vendors

Strategy

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

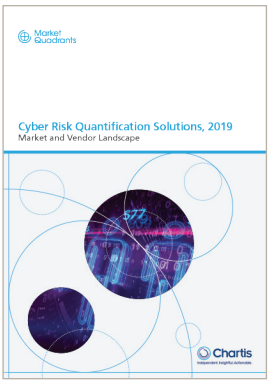
- Market analysis, including market segmentation, market demands, buyer needs, and competitive forces.
- Strategy sessions focused on aligning product and company direction based upon analyst data, research, and market intelligence.
- Advice on go-to-market positioning, messaging, and lead generation.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

Thought leadership

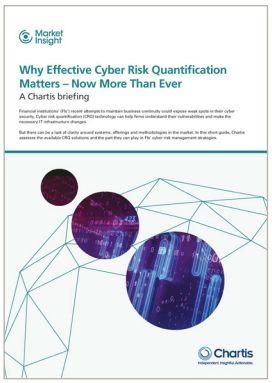
Risk technology vendors can also engage Chartis to provide thought leadership on industry trends in the form of in-person speeches and webinars, as well as custom research and thought-leadership reports. Target audiences and objectives range from internal teams to customer and user conferences. Some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

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

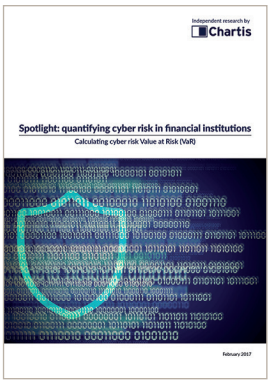
7. Further reading



Cyber Risk Quantification Solutions, 2019: Market and Vendor Landscape

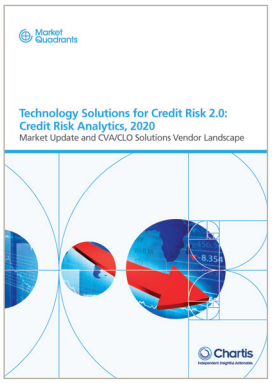


Why Effective Cyber Risk Quantification Matters – Now More Than Ever: A Chartis Briefing



Spotlight: Quantifying Cyber Risk in Financial Institutions

Enterprise GRC Solutions, 2019: Market Update and Vendor Landscape



Technology Solutions for Credit Risk 2.0: Credit Risk Analytics, 2020; Market Update and CVA/CLO Solutions Vendor Landscape

RiskTech100® 2020

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