Market Quadrants

Communications Monitoring Solutions, 2022

Market 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 management 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.
- Wealth advisory.
- Asset management.

Chartis focuses on risk and compliance technology, giving 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 developing and implementing risk management systems and programs for Fortune 500 companies and leading consulting firms.

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

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

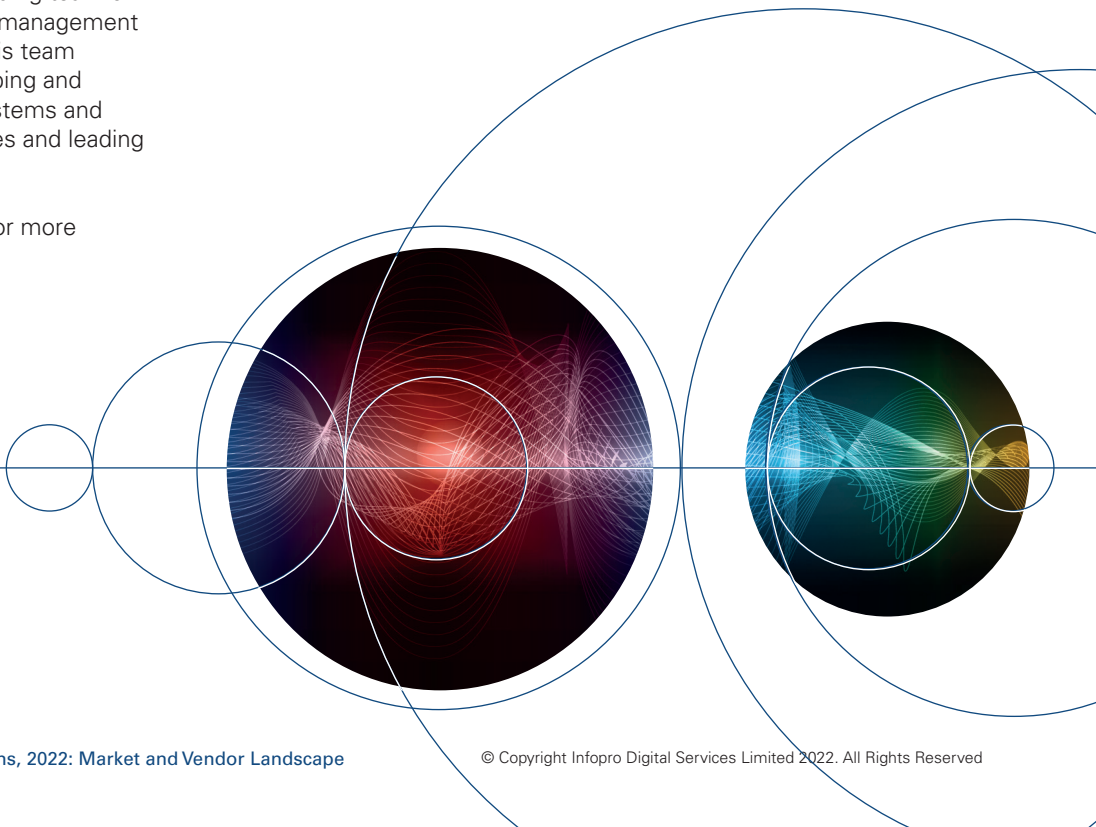


Table of contents

1. Executive summary 5

2. Market landscape 6

3. Vendor landscape 12

4. Appendix A: RiskTech Quadrant® methodology 15

5. How to use research and services from Chartis 19

6. Further reading 20

List of figures and tables

Figure 1: Financial institutions' first two lines of defense 8

Figure 2: Communications monitoring – challenges and technology solutions 11

Figure 3: RiskTech Quadrant for communications monitoring solutions, 2022 13

Figure 4: RiskTech Quadrant® research process 15

Figure 5: RiskTech Quadrant® 16

Table 1: Assessment criteria for communications monitoring solutions, 2022 12

Table 2: Vendor capabilities for communications monitoring solutions, 2022 14

1. Executive summary

Communications monitoring tools record, analyze and monitor employees' communications to mitigate risk, by identifying any internal fraud and/or breaches in regulatory requirements. Solutions collect data by recording multiple different communications channels, within and outside a financial institution's traditional tech perimeter, including emails, phone calls, instant messages and video meetings. The importance of communications monitoring has grown in the past year, driven by the COVID-19 pandemic and institutions' expanding communications requirements. Several key trends have emerged in the market:

- **Remote working at scale due to the pandemic has affected the communications monitoring landscape**. This development has been a challenge for financial institutions, which have been asked to monitor more lines of communication (including online video-call platforms) within a largely remote working environment.

- **Demands from regulators have increased**. When regulators conduct reviews or investigations, electronic communications constitute a large part of the material they request from financial firms. Regulators have issued fines to institutions that do not periodically test the effectiveness of their surveillance solutions, and to firms with an insufficient number of staff dedicated to electronic review.[1]

- **The requirements of lines of defense have changed**. The roles of the first and second lines of defense in financial firms have had to adapt to the changes caused by remote working and the pandemic. The second line of defense must now be more involved in supervising staff within the organization, rather than just those in the first line of defense.

- **Firms need more data storage and are moving to the cloud**. Regulators require financial institutions to store all communications data from recordings unedited. This data typically has been provided on 'write once, read many' (WORM) storage capabilities on physical media. Increasingly, financial institutions are using bespoke cloud solutions with defined storage capabilities, because costs for these have been dropping consistently. Publicly available options, however, may not be the cheapest; indeed, a shift toward monitoring everything may not be the best path to take. So purpose-built technology can help firms reduce costs.

Financial institutions face challenges in implementing proper communications monitoring solutions, including legacy compliance software, the introduction of new communication channels and the ability to monitor voice communications that are both complex and data-intensive. One significant challenge stems from the inability of compliance teams to ensure that remote workers do not use personal devices and communication channels to discuss any work-related matters in conversations that should be recorded.

Compounding the issue, the technology landscape for communications monitoring within financial institutions is complicated. Specific vendors provide a variety of tools, including speech-to-text conversion, natural language processing (NLP) capabilities and screen-scraping tools. As a result, many vendors in the market act as 'orchestrators', bringing together a collection of offerings within a case management or workflow solution.

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; 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 communications monitoring solutions:[2] Aiimi, Bloomberg, Fingerprint, NICE Actimize, Opsmatix, Relativity, ShieldFC, Smarsh, Spitch, SteelEye and VoxSmart.

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 responded to our requests for briefings, and some declined to participate in our research.

[1] **https://www.acaglobal.com/insights/financial-institutions-may-need-reconsider-their-approach-electronic-communication-surveillance**

[2] *Note that references to companies in this report do not constitute endorsements of their products or services by Chartis.*

2. Market landscape

Introduction and definitions

Communications monitoring tools record, analyze and monitor employees' communications. This capability covers a variety of activities that include detecting signs of suspicious behavior, insider trading and internal fraud. Tools and solutions collect data by recording and monitoring emails, phone calls, instant messages and video meetings, giving compliance teams the 'how' and 'why' information that underpins risk mitigation.

Communications monitoring: requirements

Effective communications monitoring is based on the channels of communication a firm uses (such as voice, video, messaging, etc.), and requires the technology employed to store large amounts of data.

More specific technology requirements include:

- **Reliable data**. Financial institutions' effective monitoring of communications depends on their ability to provide reliable data. Recorded material must be stored in such a way that it can be accessed easily if required. Solutions must also be able to store data in a reliable and easily accessible way.
- **Language and voice support**. Voice records may need to be transcribed using solutions that can identify and monitor many languages, including within the same communication stream. Advanced capabilities include processing low-quality audio and trader jargon.
- **Lexicons**. Traditionally, communications surveillance tools have been triggered by key words or phrases. Some firms advertise that they use 'advanced' lexicons based on former court cases and investigations.
- **Metadata analysis**. Solutions also require metadata to fill data gaps. The number of false alerts can be reduced when a solution has more information about the role, department and geography of the individuals being monitored. Additional information in metadata includes the number of participants in a conversation and whether messages are inbound or outbound.
- **Advanced analytics**. Firms employ a range of analytical capabilities, from 'fuzzy' matching and basic text analytics to more sophisticated artificial intelligence (AI) techniques, typically machine learning (ML) tools.
- **Broad channel coverage**. Several vendors claim that their solutions cover many communication channels used by staff in financial institutions. Vendors also claim that their solutions can monitor video communication channels, the use of which has grown as a result of increased remote working.

Key trends in the market

A pandemic-induced shift

The shift to remote working in the investment sector caused by the pandemic, reflecting a more general trend, created challenges for supervisory and surveillance functions (including communications and trade[3] surveillance) in ensuring that effective monitoring remained intact.

Acknowledging the challenges faced by banks, several regulators – the Commodity Futures Trading Commission (CFTC) in the US, the European Securities and Markets Authority (ESMA) in the EU and the Federal Financial Supervisory Authority (BaFin) in Germany – temporarily 'relaxed' certain record-keeping and surveillance requirements. Nevertheless, surveillance teams are likely to be highly aware of the repercussions and reputational damage that could occur if a significant incident of misconduct were to go undetected. And alongside the risk of unmonitored communications, surveillance teams are also now having to review more alerts because of the market turmoil caused by the pandemic and a spike in the number of false positives. This has placed logistical pressure on review teams working remotely to identify potential misconduct.

The biggest issue for communications surveillance systems is controlling the use of unmonitored channels (including personal cell phones, home landlines and personal communication apps) that would be banned on a trading floor. Due to restrictions around data privacy and the General Data Protection Regulation (GDPR), financial institutions may struggle to monitor these channels.

[3] *See the Chartis report* **Financial Crime Risk Management Systems: Trade Surveillance – Transaction Monitoring 2019** *for more information.*

Financial institutions must tread a fine line when addressing their communications and data monitoring. Firms face challenges in conducting the right amount of communications surveillance and ensuring that data is collected and analyzed in line with GRPR standards. On the other hand, some financial institutions may be using the records collected to monitor employee activity that may be violating privacy boundaries. In other words, firms could be seen as using either too much or too little of their employees' data.

In addition, volatility in global markets in March and April 2020 presented surveillance teams in financial institutions with significant challenges. A large increase in trades and the growing use of emails and other communication channels caused a vast increase in alerts. As a result, compliance and surveillance teams had to consider which products, assets, desks, groups and individuals to focus on, while dismissing other alerts.

In July 2020, Bloomberg indicated that use of its terminal chat platform increased by approximately 50% between Q4 2019 and the end of Q1 2020, while the average daily volume of US treasuries trades executed via voice in March and April 2020 more than doubled compared to levels in February.[4]

Regulators, having relaxed communications surveillance rules at the beginning of the pandemic, now expect staff working remotely to be monitored as closely as when they are working on the trading floor. Financial institutions in the UK have implemented several steps to follow guidelines such as 'police bankers' and 'prevent wrongdoing'. These include ensuring that staff are never alone in a room while working, enforcing limited bathroom breaks, keep an audit trail of every trade on a chat in order to preserve an audit trail, and only carrying out trades sent from authorized devices.[5]

In October 2020, the Financial Conduct Authority (FCA) put out guidance for managing increased alerts during the COVID-19 pandemic. Some additional challenges facing communications surveillance teams include avoiding the sharing of information between flatmates who work in the same industry and preventing the use of personal or unregistered devices to share confidential information. The FCA also stated that 'office and working from home arrangements should be equivalent', requiring firms to adopt new methods and technologies to mitigate risks and ensure compliance.[6]

More regulatory pressure

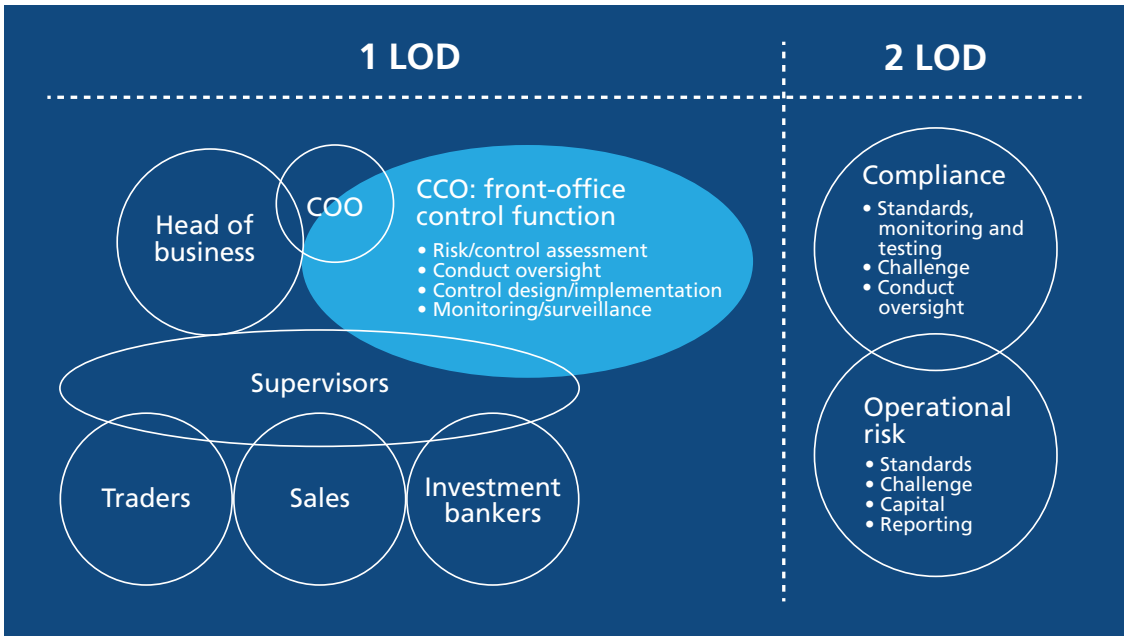
When regulators conduct reviews or investigations, electronic communications constitute a large part of the material they request from financial firms. Regulators (including the Financial Industry Regulatory Authority [FINRA]) have issued fines to institutions that do not test the effectiveness of their surveillance solutions periodically. In addition, regulators including the SEC have issued fines to institutions with an insufficient number of staff dedicated to electronic review.[7] Chartis' research has identified the following regulatory requirements for financial institutions in respect of communications monitoring and surveillance:

- **FCA**. In October 2020, the FCA stated that 'office and working from home arrangements should be equivalent' – in other words, firms should adopt new methods and technologies to mitigate risks and ensure compliance with regulations.[8] Following this, in January 2021, the FCA indicated that financial institutions must proactively review their recording policies and procedures every time there is a change in the context or environment in which their staff work. While the FCA has not placed any restrictions on the exact applications or technologies financial institutions can use, it still expects firms to ensure that their recording obligations are met.[9] [10] [11]

- **FINRA**. In October 2019, FINRA issued a report stating that firms must create and preserve, in an easily accessible place, the original versions of all communications received and sent. This includes all communication applications, such as app-based messaging services or collaboration platforms. FINRA also requires firms to continue following up red flags of potential violations of its rules and regulations.[12]

[4] **https://www.bloomberg.com/professional/blog/compliance-challenges-surge-with-messaging-during-pandemic/**
[5] **https://www.bloomberg.com/professional/blog/with-traders-far-from-offices-banks-bring-surveillance-to-homes/**
[6] **https://www.fca.org.uk/news/speeches/market-abuse-coronavirus**
[7] **https://www.acaglobal.com/insights/financial-institutions-may-need-reconsider-their-approach-electronic-communication-surveillance**
[8] **https://ukfinancialservicesinsights.deloitte.com/post/102go2k/the-future-of-work-new-challenges-for-trade-surveillance-and-good-customer-outco**
[9] **https://www.fca.org.uk/publications/newsletters/market-watch-66**
[10] **https://www.sidley.com/en/insights/newsupdates/2021/01/uk-fca-expectations-on-call-recording-in-a-remote-working-environment-market-watch-66**
[11] **https://www.sidley.com/en/insights/newsupdates/2021/01/uk-fca-expectations-on-call-recording-in-a-remote-working-environment-market-watch-66**
[12] **https://www.finra.org/rules-guidance/guidance/reports/2019-report-exam-findings-and-observations/digital-communication**

Figure 1: Financial institutions' first two lines of defense



Source: Chartis Research

- **ESMA**. In March 2020, ESMA issued a statement about financial institutions' ability to abide by Markets in Financial Instruments Directive II (MiFID II) during the pandemic. According to ESMA, firms should arrange for recordable electronic communications methods to replace telephone conversations, because of the sudden shift to working from home. ESMA did, however, recognize that in some instances, because of this shift, conversations might not be recorded. Nevertheless, it indicated that firms should provide minutes for every unrecorded call to monitor conversations and transactions. Any exceptions would be temporary, while institutions restored their recording processes as quickly as possible.[13]

Lines of defense: a shift in responsibility

Typically, communications monitoring is managed via the three lines of defense (LoDs) in financial institutions. The first LoD monitors recordings and processes data, while the second implements the technology and solutions required by the regulator (see Figure 1). The third LoD conducts an internal audit. Given that different teams in financial institutions are involved in communications monitoring, solutions must be available to each, depending on their priorities.

Markets in Financial Instruments Directive II (MiFID II)

Under this regulation, financial institutions are required to take all reasonable steps to prevent staff from making, sending or receiving telephone calls and electronic communications on devices that their companies cannot record or copy. MiFID II requires firms to retain all recordings for a five-year period and prohibits the deleting of any recording. It also stipulates that firms should have a process in place for dealing with lost or stolen devices, retention policies for devices when staff end their employment and frequent transfers of all data from devices to the institutions' databases.*

***https://www.algoodbody.com/insights-publications/esma-announcement-on-mifid-ii-requirements-for-telephone-recordings**

More recently, financial firms have been required to update the policies, procedures and responsibilities of the first and second LoDs to deal with remote working. A key requirement is that the first and second LoDs must be proactive in managing risk and remain in close contact to ensure they are not working at cross purposes.

This has encouraged a shift in responsibility for communications monitoring, which increasingly is shared between the operations and compliance departments. Systems should be able to account for the priorities of both when it comes to monitoring and response requirements.

[13] **https://www.algoodbody.com/images/uploads/services/Financial/esma35-43-2348_esma_statement_on_covid-19_telephone_recording1.pdf**

Increased demand for communications data storage and the move to the cloud

Financial firms are looking for ways to store their communications surveillance data. Regulators do not permit firms to edit or alter recordings, and maintaining the large storage requirements required for voice, image and video files is making in-house data storage increasingly costly. In addition, communications surveillance data is often unstructured.

Financial institutions have shown an increasing willingness to swap traditional in-house data storage solutions for cloud options. This has been made possible by the data storage security offered by large cloud providers. While this approach presents its own risks (at a basic level, that of being on a relatively centralized system), many financial institutions regard cloud security as having key advantages over security provided in-house. Notable among these are an ability to geofence data and convert information into write-only formats.

Increasingly, cloud data solutions provide these services at lower cost and higher efficiency. Another key selling point for these solutions is their rapid deployment capabilities.

The challenges facing financial institutions

Financial firms face several challenges in ensuring effective communications monitoring:

- **Large numbers of false positives**. This is undoubtedly the single biggest challenge facing institutions attempting to monitor their communications. Individuals communicate with each other in a huge variety of often complex ways, and there are limits to what technology can accomplish in attempting to assess whether they are violating internal rules or external regulations. While monitoring systems can parse for prohibited words or phrases, or even analyze sentiments, they will never be able to fully capture the nuance of human expression. False positives are a reality, therefore, and a common benchmark in communications monitoring, as many solutions focus on reducing them. Analytics that can reduce false positives effectively are at a premium.
- **A wider array of communication channels**. Communications monitoring systems have a growing array of channels to monitor (including online video-based communication platforms). Financial institutions require monitoring solutions that can operate across platforms.
- **Ensuring effective voice surveillance**. Voice-monitoring channels should be able to capture and aggregate diverse voice channels (including phone lines and apps), eliminating background noise without compromising accuracy and storing voice data so it can be retrieved easily.
- **Recognizing and transcribing speech**. Regulators have increased expectations of financial institutions' ability to conduct voice surveillance, and firms want to ensure a high level of speech to text accuracy. Challenges in this area include dealing with mixed languages, using coded speech, understanding traders' terminology and jargon, assessing voice biometrics (can a trader or individual be identified by their voice?) and detecting intent.
- **Monitoring 'dark' channels**. Numerous communication channels, mobile devices and encrypted messaging services have made it easier for individuals to share information without detection. In addition, the move to remote and hybrid working has made monitoring more challenging for regulators and compliance teams. Some traders use 20 to 30 different platforms, which can have different protocols and data formats that are difficult to capture with one solution.[14]
- **Employing usable analytics**. For financial institutions, implementing ML in communications surveillance solutions is not easy, requiring considerable financial investment, people, data and training, and with potential impacts on other parts of the business. Different departments and individuals are also subject to different types of risk, a dynamic that should be reflected in communications monitoring solutions.
- **Inadequate infrastructure**. Before the broad shift to remote working, financial institutions' compliance infrastructure did not cover channels that previously were used only 'occasionally' but that became core communication methods during the pandemic.[15]

[14] **https://a-teaminsight.com/trading-electronic-communications-surveillance-in-a-changing-world/?brand=tti**
[15] **https://www.verba.com/communication-compliance-blueprint-2021-financial-services-perspective/**

The data management challenge

Data management remains a key issue for most risk management or compliance functions, and communications surveillance is no exception. Specific challenges include:

- **Risk systems require good quality data**. Regulators have indicated that firms' data integrity controls will feature heavily on their agendas. Systems that rely on rules engines and statistical analysis often require data in specific formats, and high-quality data is essential for analysis.

- **Mapping data across the organization is a complex undertaking** but is necessary for broader surveillance. Lists and sub-lists of individuals may be held in a single location or in several places. Certain lists – such as those used to prepare annual reports and accounts, or to support debt issuance – may be held in centralized HR systems. Others may be held in corporate banking, investment banking and market divisions, and are often transaction-specific. Devising a reliable way to map all the relevant data needed for surveillance purposes, and then keeping these maps updated, can be a significant challenge.

- **Handling Big Data**. For financial firms, finding ways to query and surface the data they need from an increasingly varied and amorphous data environment can be a major challenge. The e-comms data that firms process, for example, can come in relational, structured formats (typically in row and columnar databases), semi-structured formats (e.g., weblogs, social profiles and XML) or completely unstructured formats (e.g., images, audio or pdf documents).

Integrating with trading systems – a work in progress

Communications monitoring is often an integral part of the trade surveillance process (something Chartis has discussed previously[16]). This dynamic continues to inform how communications monitoring evolves. Trading institutions and capital markets firms have focused on capturing information around the trade lifecycle, including communications and trade information. One of the main drivers for this is the requirement for trade reconstruction mandated by such regulations as Dodd-Frank, the Market Abuse Regulation (MAR) and MiFID II. This necessitates data that includes emails and SMS messages.

Communications should be viewed in the context of trade systems and should be coupled with unstructured data and metadata that includes relationship documentation and information from audit and compliance departments.

However, trade and communications surveillance are typically run by different teams (such as operations and compliance), with different priorities and technology. Bringing both forms of monitoring under one team and using one solution may be difficult in many firms because of differences in the teams' responsibilities and requirements.

The conflicting requirements and capabilities of compliance and trading teams, and their different technology architectures, mean that combining trade and communications data to generate alerts is still relatively rare in financial firms. Nevertheless, trade reconstruction is a requirement under regulations such as MIFID II.[17] This seldom uses 'combined analytics', in the sense that a risk score will have a combined qualitative outcome from both the communications

Filtering alerts

The most common communications monitoring technique is the use of *lexicons*, or pre-determined sets of words and phrases, that trigger alerts for review by compliance officers. Lexicons contain such information about communications as the job role, department, location and language of the people involved in the conversation, as well as the number of participants. This information enables the compliance team to assess the risk or accuracy of the alerts. So, for example, an insider-trading alert on a staff member who does not have access to inside information could be disregarded. The use of metadata can also make the surveillance process more effective and efficient.

To enhance the effectiveness of communications surveillance, firms can use AI, ML and pre-trained models to detect misconduct more effectively and generate risk alerts. These can:

- Identify irrelevant and duplicate data, reducing false alerts.
- Learn by reviewing former alerts.
- Identify languages and phrases that previously were ignored.
- Create new models built on past examples.

[16] *'Financial Crime Risk Management Systems: Trade Surveillance – Transaction Monitoring 2019; Overview and Vendor Landscape'*
[17] **https://www.esma.europa.eu/sites/default/files/library/2016-1452_guidelines_mifid_ii_transaction_reporting.pdf**

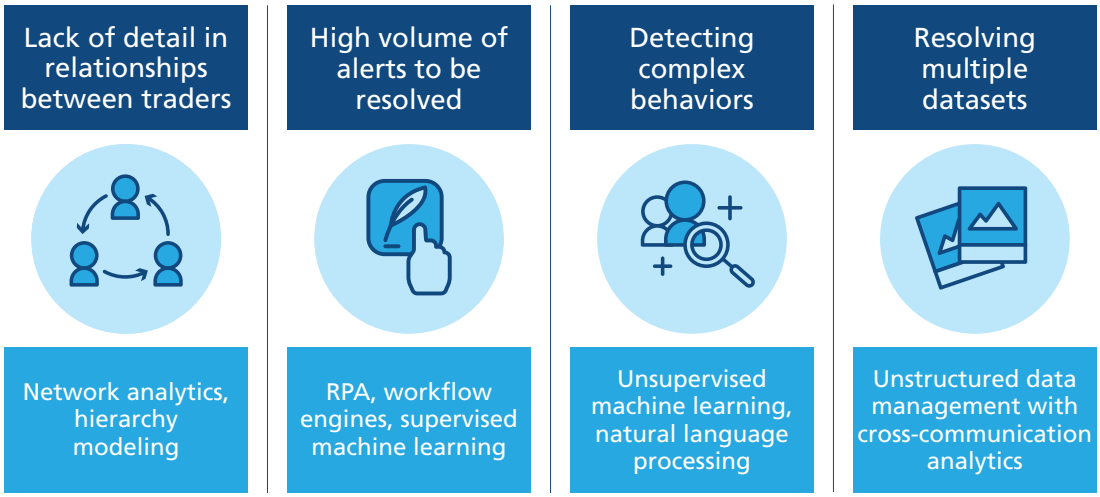
surveillance and trading sides of the business. But firms looking to address this challenge should be able to present information from trading and surveillance systems in a unified way.

Using technology to address the challenges

Figure 2 identifies some of the key challenges in the communications monitoring landscape, and the relevant technological solutions for each.

Because of the variety of challenges and solutions, the vendor landscape for communications monitoring is correspondingly complex.

Figure 2: Communications monitoring – challenges and technology solutions



Source: Chartis Research

3. Vendor landscape

The vendor landscape for communications monitoring is particularly diverse, featuring a variety of players and capabilities. Third parties are often used to provide individual capabilities within a specific solution, including NLP for analyzing text, speech analytics and screen-scraping.

As a result, the communications monitoring landscape often involves an array of vendors, with orchestration layers and workflows bringing together disparate communications monitoring capabilities and/or analytics. As such, the concept of a 'communications monitoring' vendor can be relatively fluid. Nevertheless, vendors can be categorized into approximate groupings – one distinguishing factor is the divide between investigative and detection capabilities.

Investigation occurs when an abuse or contravention has been detected within a system (by a trade surveillance tool, for example, or via an external event such as a report to HR). The system is then required to review and analyze any communications around the incident. These solutions therefore prioritize several elements of the process:

- The analysis of multiple communication channels within the same dashboard.
- Metadata and network analysis, to determine connections between communicating entities.
- Storage and retrieval capabilities.
- Integrations with other systems, such as trading or transaction monitoring (for trade reconstruction, for example).

Detection tools typically are used to detect when abuse has occurred – they sit 'in stream' with the communications channel and are designed to catch contraventions as they happen. They:

- Prioritize real-time analytics and streaming.
- Are primarily (but not always) focused on a single channel, such as voice, email or chat.
- Prioritize sentiment analysis to determine 'intent'.

Vendors typically focus on one of these, although larger and more complex enterprise solutions can feature more.

Chartis RiskTech Quadrant and vendor capabilities for communications monitoring solutions, 2022

Figure 3 shows the RiskTech Quadrant for communications monitoring solutions, 2022. Table 1 lists the criteria we used to assess the vendors, while Table 2 lists the vendor capabilities in this area.

Quadrant dynamics

The various vendors in the RiskTech Quadrant for communications monitoring have differing key focus areas, as highlighted in Table 2. There are, however, firms with mature, enterprise offerings: those with orchestration or enterprise workflow

Table 1: Assessment criteria for communications monitoring solutions, 2022

Completeness of offering	Market potential
• Data transformation	• Client growth
• Audio and voice analytics	• Market strategy
• NPL and document analysis	• Growth strategy
• Search capacity	• Business model
• Detection analytics	• Financials
• Scalability and infrastructure	

Source: Chartis Research

Figure 3: RiskTech Quadrant for communications monitoring solutions, 2022

Source: Chartis Research

capabilities – and more specifically, those that can manage a wider array of communications – have tended to appear toward the upper right of the quadrant. This does not necessarily make those firms the vendors of choice for many financial institutions. Less regulated or smaller firms with less stringent requirements to view all communications within a single dashboard may instead opt for a best-of-breed or point solution at a lower price point to enable specialist capabilities.

Table 2: Vendor capabilities for communications monitoring solutions, 2022

Vendor	Data transformation	Audio and voice analytics	NPL and document analysis	Search capacity	Detection analytics	Scalability and infrastructure
Aiimi	****	**	***	***	**	**
Bloomberg	**	**	****	****	**	***
Fingerprint	****	***	***	***	**	***
NICE Actimize	***	****	***	***	****	**
Opsmatix	**	**	**	***	**	****
Relativity	****	****	***	***	****	**
ShieldFC	**	***	****	****	****	**
Smarsh	***	****	***	***	****	**
Spitch	**	****	*	****	***	***
SteelEye	****	****	**	****	**	****
VoxSmart	***	***	***	****	*	***

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

4. Appendix A: RiskTech Quadrant® methodology

Chartis is a research and advisory firm that provides technology and business advice to the global risk management industry. Chartis provides independent market intelligence regarding market dynamics, regulatory trends, technology trends, best practices, competitive landscapes, market sizes, expenditure priorities, and mergers and acquisitions. Chartis' 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 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.

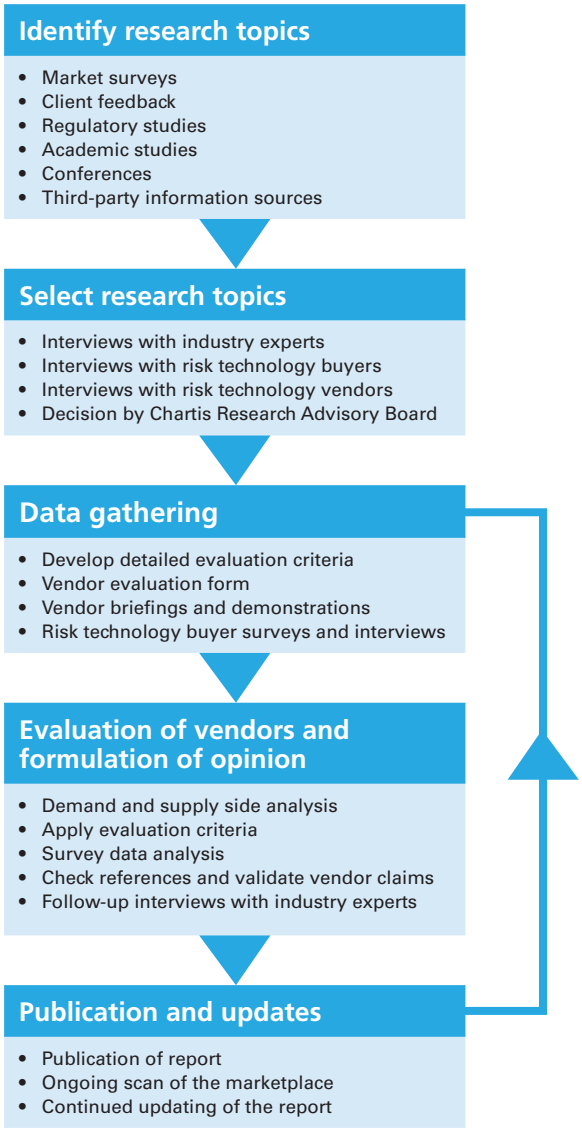
Inclusion in the RiskTech Quadrant®

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 4 below describes the research process.

Figure 4: 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.

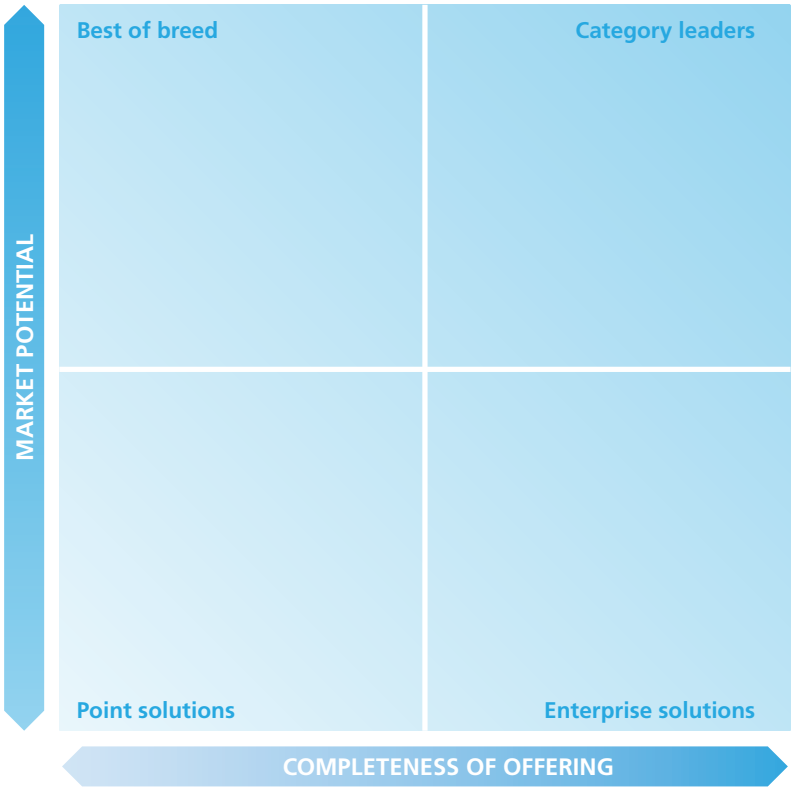
Evaluation criteria

The RiskTech Quadrant® (see Figure 5) evaluates vendors on two key dimensions:

1. Completeness of offering

2. Market potential

Figure 5: 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 number 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 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 varies for each

subject area, but special attention is 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.

5. How to use research and services from Chartis

In addition to our industry reports, Chartis offers customized information and consulting services. Our in-depth knowledge of the risk technology market and best practices 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.

Advisory services

Advisory services and tailored research provide a powerful way for Chartis clients to leverage our independent thinking to create and enhance their market positioning in critical areas.

Our offering is grounded in our market-leading research, which focuses on the industry and regulatory issues and drivers, critical risk technologies and leading market practices impacting our sector. We use our deep insight and expertise to provide our clients with targeted market and industry analysis, tailoring content to assess the impact and potential of relevant regulatory and business issues, and highlighting potential solutions and approaches.

Chartis' advisory services include:

Market dynamics

The markets that our clients – vendors, institutions and consultants – address are changing at an ever-increasing pace. Understanding the market dynamics is a critical component of success, and Chartis uses its deep industry and technical knowledge to provide customized analysis of the specific issues and concerns our clients are facing.

Market positioning

In today's highly competitive market, it is no longer enough simply to have a leading product or solution. Buyers must be able to appreciate the differentiating capabilities of your brand and solutions, and understand your ability to help them solve their issues.

Working with our clients, we generate compelling, independent co-branded research, targeting critical business issues. This helps our clients to position their solutions effectively, 'own' key issues and stand out from the crowd.

Collaborating closely with our clients, we develop pragmatic, resonant thought-leadership papers with immediate industry relevance and impact.

Our offerings include:

- **Co-branded research** on key market topics to provide a unique and compelling point of view that addresses a key industry driver and highlights the relevant issues. Reports can be tailored to varying levels of depth and can be powered by quantitative survey fieldwork, qualitative industry interviews, our deep domain expertise or a blend of all three.
- **Chairing roundtables and/or facilitating events and workshops** to support clients in hosting compelling events that put them at the heart of the discussion.
- **Targeted marketing through our sister brands**, leveraging the power of our parent group – Infopro Digital – to reach across leading brands such as Risk.net, WatersTechnology, FX Week and Central Banking.

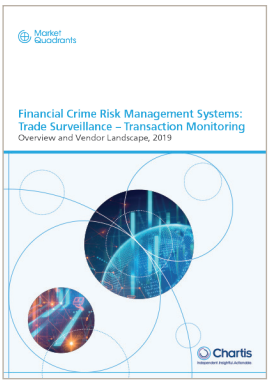
Competitor analysis

Our unique focus on risk technology gives us unrivalled knowledge of the institutions and vendors in the sector, as well as those looking to enter it. Through our industry experts, Chartis clients can tap our insights to gain a much deeper understanding of their competitors and the strategies they should pursue to better position themselves for success.

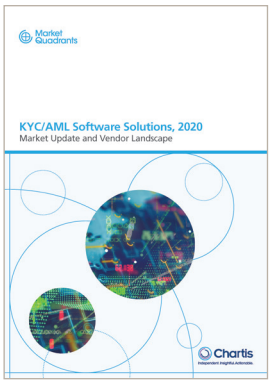
Regulatory impact analysis

The analysis and assessment of regulatory change and implementation is one of Chartis' core strengths. We can apply our insights to assess the impact of change on the market – either as it applies to vendors and the institutions they serve, or on a client's specific product and customer base. We can also provide insights to guide product strategy and associated go-to-market activities, which we can execute for internal use to drive our clients' strategy or as a co-branded positioning paper to raise market awareness and 'buzz' around a particular issue.

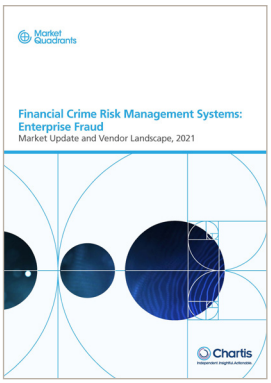
6. Further reading



Financial Crime Risk Management Systems: Trade Surveillance – Transaction Monitoring 2019

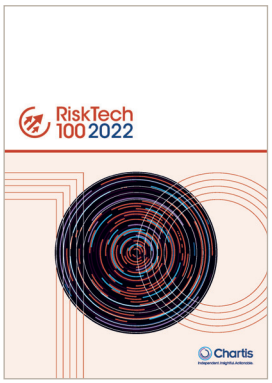


KYC/AML Software Solutions, 2020: Market Update and Vendor Landscape

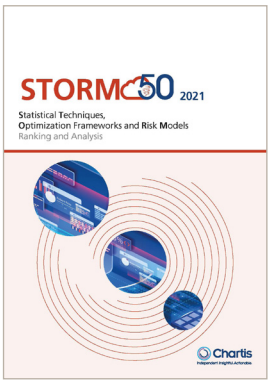


Financial Crime Risk Management Systems: Enterprise Fraud; Market Update and Vendor Landscape, 2021

Big Bets 2022



RiskTech100® 2022



STORM50 2021

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