Market Guide for Supplier Risk Management Solutions

Published 16 May 2022 - ID G00740032 - 21 min read

By Analyst(s): Koray Kose, Cian Curtin

Initiatives: Supply Chain Technology Strategy and Selection; Procurement and Strategic Sourcing Applications; Procurement Functional Enablement; Sourcing and Procurement

As economies emerge unevenly from the impacts of the pandemic, concerns about supplier viability, cybersecurity and more abound. This research will help supply chain technology leaders identify prospective solutions to monitor, manage and mitigate supplier risk.

Overview

Key Findings

- The 2020 Gartner Future of Supply Chain Survey found that 87% of respondents were planning to invest in the next two years to make their supply chains more resilient. This finding was proven accurate, as the 2021 Gartner Supply Chain Risk and Resilience Survey showed at least 75% of supply chain companies have either implemented or are implementing a risk management organization, with 52% reporting dedicated supply chain risk roles at the global strategic level.

- The software market to address supplier risk remains highly fragmented, leaving companies with almost too many options.

- Users of technology can monitor and analyze supplier risk events in real time or near real time. However, more sophisticated use cases, which are driving solutions to be predictive and prescriptive using artificial intelligence (AI), machine learning and other emerging technologies, are still being developed.

Recommendations

Supply chain technology leaders supporting supplier risk should:

- Make technology a foundational part of their supplier risk management program, but understand that it's not a panacea for eliminating vulnerabilities from risks. But technology is quickly becoming a requirement to enable risk management to avoid, absorb and recover from risk events as a competitive advantage.
- Prepare to use a combination of solutions of foundational systems with specialized software providing AI and machine learning (ML), advanced analytics and depth of quality data augmenting master data management, supplier collaboration, operations excellence in sensing and responding, hence resilience. This is critical to avoid overinvestment into redundancies, or into single solutions that are not built to cover comprehensive risk management. The fragmentation of the solutions market requires careful assessment of the needed capabilities to be matched with the offerings.
- Match the technology to the types of risk being managed. Many types of vendors address risk, but not all of them address the same types of risk. Additionally, there are functional differences between technologies that evaluate risk based on historic patterns and date, monitor risks based on real-time data, and intelligently predict risk and help to mitigate risk. No one technology solution can cover every single type of risk that affects suppliers.

Market Definition

Supplier risk management is core to end-to-end supply chain risk management and aims to make businesses resilient to risks across the physical and digital supply ecosystem. It is strengthened by technology used for risk identification and monitoring, holistic risk impact analysis and coordinated operational and strategic risk management. Additionally, supplier risk management is not synonymous with third-party risk management (TPRM), which is broader in scope and definition. TPRM goes beyond an arm's length relationship (e.g., includes regulators, subcontracted service providers and other partners) and typically does not link real-world events to supply chain impacts. This Market Guide does not feature any companies that are purely services or consultancies, market risk or geopolitical risk advisors. However, service providers may also prove useful in monitoring, managing and mitigating supplier risk.

Market Description

Supplier risk management is a key competitive advantage. Enhanced risk management enables sourcing and procurement professionals to impact a company's continued success from product development, implementation to phase out. Ability to create resilience and tackle predictable and unpredictable shocks, changes in legislation, managing supplier performance, logistics and financial risks, ESG and CSR, cybersecurity and capacity fluctuations is critical. Technology is a key enabler for success in managing complex, comprehensive and time-sensitive data. Supplier risk is best managed by complementing a sourcing suite with best-of-breed technology that integrates well and can tackle (un-)structured, fluid data in fast- paced and fragile environments. Investments into risk management have increased by 30% (based on % on direct material spend) from 2021 to 2022. [1]

Supplier risk comprises a variety of risks; however, this Market Guide will focus on the following seven common categories (see Figure 1):

- **Risk Event Monitoring** — Refers to supply chain disruptions caused by weather, geopolitical events and other hazards. Events are linked in real time or near real time to suppliers and supply chain transactions that are at risk (e.g., orders, shipments, manufacturing). Risk event monitoring includes the ability to map the impact visually to gauge the impact to the suppliers and how it may affect orders. Sourcing and procurement professionals can use this information before placing orders or to reallocate unfilled orders. Event monitoring may also prove useful to other supply chain roles, including logistics and transportation managers, who may use the same platform. This Market Guide will focus on the sourcing and procurement professional.
- **Financial** — Identifies the financial viability of a supplier, and whether the supplier is currently experiencing, or likely to experience, any financial issues that will impair its ability to fulfill obligations toward an organization and its own supply chain.
- **Corporate social responsibility (CSR)** — Enables companies to track and manage corporate goals, improving their impact on social and environmental goals. CSR combines supplier compliance with legal, ethical, safety and social compliance as a baseline, with the ability to contextualize the company's focus (e.g., into supplier diversity, carbon footprint, modern slavery, conflict minerals). CSR may be linked to environmental, social and corporate governance (ESG) reporting, but since it is not baselined solely on legislation, it comes in many more varieties and specialties.

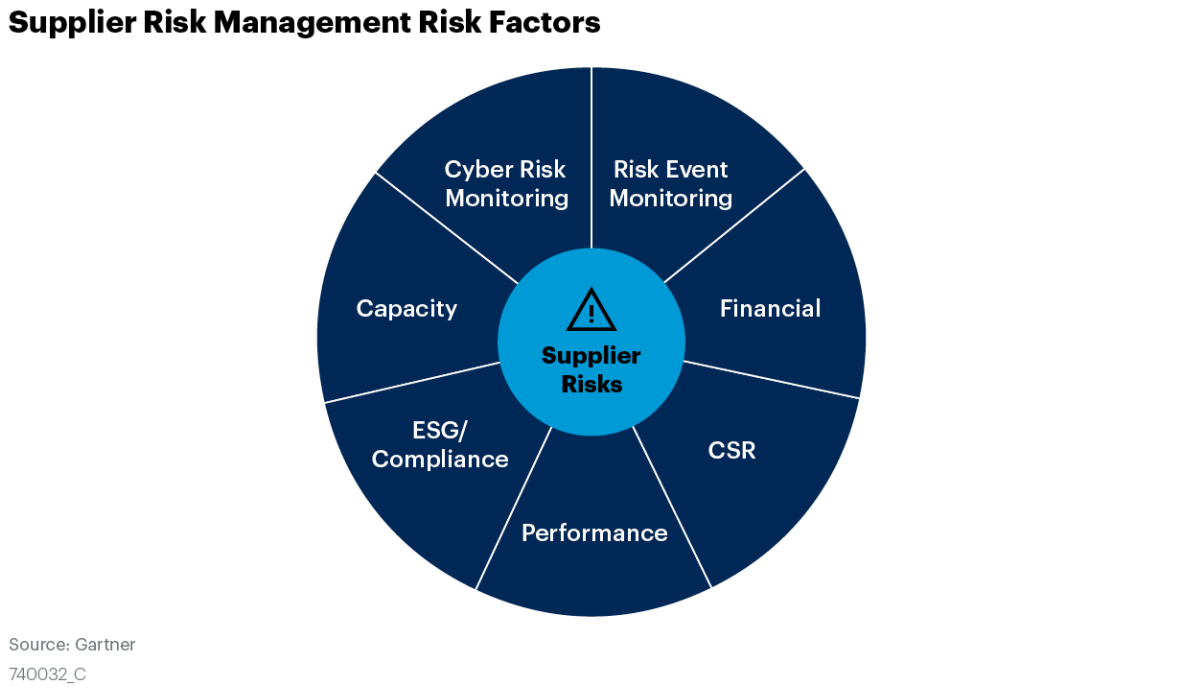
- **Performance** — Creates and manages supplier performance dashboards that can track many metrics, including risk, to provide a holistic supplier view. Examples include quality metrics, logistics metrics (e.g., on-time delivery performance), payment metrics, as well as key risk indicators, such as vesting balance, spend concentration and financial strength. These modules are often part of broader strategic sourcing suites.

- **Compliance/ESG** — Refers to regulatory and compliance mandates often managed by a category of software called third-party risk management. Some vendors can address both. This type of functionality is often used by legal, compliance and finance departments to check all third parties (not just suppliers) against anti-bribery, anti-money-laundering, restricted party screening lists, background checks and more. It can also include monitoring compliance to other government agency requirements (e.g., U.S. Office of Foreign Assets Control, U.S. Food and Drug Administration, U.S. Department of Agriculture).

- **Capacity** — Refers to what end users often cite as a top risk when mentioning suppliers. However, capacity is not easily solvable through risk software. Supplier collaboration hubs (e.g., E2open, SupplyOn, SourceDay) and supply chain planning applications (e.g., Kinaxis or o9 Solutions) often prove more useful in mitigating supplier capacity issues. But some sourcing-oriented platforms can offer some visibility into potential capacity issues, usually by tracking current order status, performance against order history, supplier responses and acknowledgments.

- **Cyber risk monitoring** — Refers to the ability to evaluate a supplier's or prospective supplier's cybersecurity capacity and resilience. Cyber risk monitoring also tracks cyber risk events and suppliers adherence to cyber governance policies and certifications through surveys. This is not the same as cybersecurity, which refers to the people, policies, processes and technologies employed by an enterprise to protect its cyber assets (e.g., IT security, Internet of Things security, information security and operational technology security, and can respond to attacks/hacks to contain, protect and resecure information). Cyber risk monitoring is separate from risk event monitoring because it is a purely defensive resilience evaluation and monitoring effort against intentional attacks to access intangible assets (e.g., data and information) that are essential for an organization's operations. Risk event monitoring vendors, since embedding critical and sensitive company data, should also be evaluated by cyber risk monitoring vendors as part of the client's supplier portfolio. Every vendor where an organization's information is used, stored and created is within scope for checks for cyber risk. A key difference for risk event monitoring, yet showing signs of ongoing integrations, is that risk event monitoring looks into physical supply chain disruptions that are often unintentional and not targeted onto their organization, whereas cyber risk monitoring searches for "intentional" attacks on the organization's intangible assets (or the intangible assets of one of its vendors or to impede its operations).

Figure 1: Supplier Risk Management Risk Factors



Source: Gartner
740032_C

Gartner

Market Direction

Gartner has seen a resurgence in inquiries for supplier risk management technology in response to the risk events in the last two years, such as the pandemic, the semiconductor crisis and the Russian invasion of Ukraine. As a result, many vendors are positioning themselves as the leader of supplier risk management solutions. To illustrate this point, ask someone, "How do you define supplier risk?" You're likely to receive a wide variety of responses. Several trends currently affect the supplier risk management solution market:

- **Focus on resilience:** Recent risk events have brought renewed interest in the supplier risk management solutions market. But as many companies have come to terms with the new reality of expecting the unexpected, the focus is shifting to how best to prepare one's supply chain to deal with future shock events, or better, how to manage them more effectively than the competition. Supplier risk management solutions can support the sourcing strategy by identifying key suppliers, components or geographies at risk. The solutions should also link to actual supply chain transactions (e.g., orders, work in progress, shipments) to measure value at risk.

- **Transformation of supply chains into supply networks and ecosystems:** Companies have very little control over the frequent rate of new risk events, but they do control the setup of their supply network and chains. An ongoing desire to create resilience is driving the need to transform supply chains into networks and ecosystems with strategic redundancies in a multipolarized future. Visibility into the supply chain is key for transformation success. To achieve visibility, technology is the foundation. Ultimately, control towers that enable the management of the multienterprise business network need risk data and risk technologies to feed complex interdependent scenarios in an easy-to-manage framework (see also Magic Quadrant for Multienterprise Supply Chain Business Networks).

- **Increasing frequency of cyberattacks:** Supply chain cyberattacks continue to occur and are only growing. Attacks on organizations in critical infrastructure sectors have increased dramatically, from fewer than 10, in 2013, to almost 400, in 2020 — a 3,900% change. [2] In response to the Russian invasion of Ukraine, NATO governments are already moving to prepare for cyberwar via dedicated cyberdefense units. However, we clearly see spillovers into the "physical" supply chain, recent examples include the cyberattacks on Colonial Pipeline and JBS Foods. Failure can be crippling. There is a wide variety of highly undesirable outcomes that can result from a supply chain susceptible to a cyberattack. These include disruption of the actual operation of the supply chain, significant damage to brand and reputation, impact on product safety and integrity, loss or theft of intellectual property, and substantial fines and fees.

- **Increasing incorporation of AI/ML:** Historically, risk management solutions have been either historical in nature or built to monitor events in real time. Embedded AI/ML gives solution providers the ability to offer customers more refined financial risk scores, better impact modeling and the beginnings of predictive analysis. According to a recent Gartner survey, when asked what tactics they use to manage supply chain disruptions, 45% of respondents stated they currently use predictive analytics to identify and monitor disruptive events, including supplier risk events. [3]

- **Expanding emphasis on compliance risk:** There are increasing compliance requirements that companies are looking to supplier risk management solutions to support. For example, the German "Due Diligence Act" on corporate responsibility in supply chains, comes into full effect at the start of 2023 with associated penalties for noncompliance. This trend is being adopted by other countries and larger supranational institutions as well, and includes the pan-European Sustainable Corporate Governance proposal and the Uyghur Forced Labor Prevention Act in the U.S.

- **Need for supplier visibility:** Gartner is starting to see an overlap between inquiries about supplier risk and supplier mapping. Supplier risk management solutions are not meant to function as network modeling tools, nor do they create a digital twin of the supply chain. Most supplier risk solutions can monitor risk to the subtier level, provided the customer supplies the tool with those relationships. The vendors that help find these relationships are the exception and are only truly effective when utilizing emerging technologies, like graph technology and blockchain. According to Gartner's Risk and Resilience study from 2021, 70% of companies ranked improving supplier visibility among their top three of most important areas to focus.

Market Analysis

Supplier risk management solutions need to support the following abilities:

- **Monitor** — Provide visibility into risk events through dashboards, reports, maps, alerts and notifications.
- **Analyze** — Measure the potential impact to a customer's suppliers and provide an impact summary.
- **Manage** — Provide functionality to support risk management efforts through measurable action plans, workflow and recommendations.
- **Learn** — Apply ML to fine-tune future recommendations and impact analysis.

In addition to the core capabilities listed above, there are additional important evaluation criteria. Supplier risk solutions should also be evaluated based on following factors:

- **Robust partner ecosystems** — No one vendor can cover all types of risk equally well. Additionally, many companies have already invested in various ERP, sourcing or supply chain systems that need to integrate and work with risk solutions. Supplier risk solution providers need to partner or at least integrate with weather services, financial reporting services, CSR rating services, cybersecurity platforms, sourcing applications, ERP systems and more.
- **Integration methodology and capabilities** — Providers need to be able to connect through EDI and APIs and have standard templates for integrating to common back-end systems. Additionally, providers may also have to incorporate IoT data as asset tracking becomes more prevalent.

- **Advanced analytics** — Advanced analytics doesn't refer to only dashboards and reports, although they are part of it. It also refers to the concept of embedding the insight generated by the analytics engine into the screens and workflows of the system user. In other words, in the real-time world of event monitoring, sourcing and procurement professionals don't have the time to submit a request to the IT team for a report that sits in a queue for two weeks. The information needs to be available immediately in the screens and dashboards already being used by the business owner. Dashboards need to be both visual and convey top-level information as well as offer drill-down capabilities to get to the transactional data, which is still often rendered in list format.

- **Data quality** — Refers to the supplier information, which is often the responsibility of the customer, as well as the quality of the risk events measured and their correlation and appropriateness to the customer's supply chain. Data quality also refers to the preciseness of the information. For example, it's not good enough to only track the headquarters of a supplier if manufacturing is happening at a different site altogether. Actual sites and nodes need to be tracked.

- **Supplier discovery** — Most supplier risk management platforms are not meant to function as supplier discovery tools, but some providers are looking at ways to support this use case. It requires a multitenant architecture and commercial agreements that allow for the sharing of basic, noncompetitive information, as well as AI and/or ML, to analyze the appropriateness of a potential new provider.

- **Supplier visibility and mapping** — Most supplier risk management platforms are not meant to function as modeling tools or supplier relationship management tools. However, more companies are demanding this type of functionality from their risk provider, and it makes logical sense. How can companies truly measure risk if they don't have the ability to measure it down to the nth tier of their supply chain and map it continuously (not only one point in time)?

- **Value at risk** — A supplier risk management platform is of limited value if it can't tell how much value is at risk. Unfortunately, not every provider can link the external risk events to actual supply chain transactions (e.g., orders, shipments, work in progress). Even when the provider's platform can, it requires additional integration and cost, which often makes the overall investment seem not worth the time or money. However, this link is necessary to be able to react to events in a timely manner.

- **Multitenant architecture** — Most supplier risk management solutions are cloud-based, but not all of them use a multitenant architecture where customers are on the same version of the application and have access to community-generated intelligence. For example, without this type of architecture, any analysis of risk will only look at a company's own data and not any additional elements created by the community at large. In addition to this type of architecture, the vendor would need to have the proper commercial terms in their contracts in place to allow for the use or sharing of community-generated but nondisclosing information.

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

Market Introduction

We've categorized the vendors by the major types of risk they support natively (i.e., not through partners). For example, only vendors that source financial information themselves are given credit for addressing financial risk. These vendors often partner with broader suite vendors that would not receive an X unless they also function as a primary source of financial information. This is why buyers should prepare themselves for considering more than one solution to meet their supplier risk management needs.

Table 1: Supplier Risk Management Vendors by Area

(Enlarged table in Appendix)

Vendor	Event Monitoring	Financial	CSR	Performance	Compliance/ESG	Capacity	Cyber Risk
Achilles		X	X		X		X
apexanalytix	X	X	X	X	X		
Aravo	X			X	X		X
Coupa				X	X	X	X
Darkbeam							X
Dun & Bradstreet	X	X			X		
EcoVadis			X				
Elementum	X						
Everstream Analytics	X				X		X
HICX				X	X		
IntegrityNext			X		X		
Interos	X				X		X
Ivalua				X	X	X	
JAGGAER				X	X	X	
Oracle				X	X		
NQC			X		X		X
RapidRatings		X					
Resilinc	X			X		X	X
riskmethods	X			X			X
SAP Ariba	X			X	X	X	
SupplierGATEWAY			X		X		
SupplyShift			X		X		
Zycus				X		X	

Source: Gartner (May 2022)

Table 2: Supplier Risk Management Vendors' General Information

(Enlarged table in Appendix)

Vendor ↓	Headquarters Location ↓
Achilles	Abingdon, U.K.
apexanalytix	Greensboro, North Carolina, U.S.
Aravo	San Francisco, California, U.S.
Coupa	San Mateo, California, U.S.
Darkbeam	Bristol, U.K.
Dun & Bradstreet	Short Hills, New Jersey, U.S.
EcoVadis	Paris, France
Everstream Analytics	San Marcos, California, U.S.
HICX	London, U.K.
IntegrityNext	Munich, Germany
Interos	Arlington, Virginia, U.S.
Ivalua	Redwood City, California, U.S.
JAGGAER	Morrisville, North Carolina, U.S.
Oracle	Austin, Texas, U.S.
NQC	Manchester, U.K.
RapidRatings	New York, New York, U.S.
Resilinc	Milpitas, California, U.S.
riskmethods	Munich, Germany
SAP Ariba	Palo Alto, California, U.S.
SupplierGATEWAY	Santa Ana, California, U.S.
SupplyShift	Santa Cruz, Californiav
Zycus	Princeton, New Jersey, U.S.

Source: Gartner (May 2022)

Market Recommendations

Risk management professionals should tread very carefully into the supplier risk management marketplace. Many companies are convinced that a technology vendor and solution will provide the complete answer to their risk management challenges. However, those that lead with technology most often suffer from inflated expectations and unmet risk management needs. It is imperative that companies design and build a solid framework and set of metrics before evaluating a supplier risk management vendor. Supplier risk management initiatives must include input from groups outside the supply chain function, including legal, finance, IT and others. Survey your current landscape for applications that may provide a role in supplier risk management.

We recommend following these steps prior to engaging in the search for supplier risk management software vendor:

1. Establish a cross-functional team tasked with creating a risk framework to support risk-based decisions.

2. Brainstorm potential supplier-related risks that could impact the business include known frequent risks and unknown catastrophic scenarios likewise.

3. Rate risks to create a prioritized list of business risks.

4. Plot a risk tolerance frontier based on the organization's risk appetite and test its current resilience to distill gaps.

5. Create risk mitigation plans and the layout of critical capabilities that will close identified gaps by type of risk, resilience, risk appetite and supplier tier.

Once these steps are in place, you can proceed with the software selection process. To identify the most suitable software vendors:

- Match prioritized risks and critical capabilities to the list of software providers.
- Use a best-of-breed approach when you are targeting a tool that can complement your existing sourcing suite when evaluating providers. Select a sourcing suite with "risk capabilities" when you are seeking to replace your current sourcing suite, yet sourcing suites with risk capabilities often provide less depth and emerging technology capabilities for managing risk.

- Identify how your risk management project fits into your overall IT infrastructure and future strategy. Keep a forward-looking focus instead of solely trying to fix today's problems. For example, do you want your supplier risk capabilities to stand alone, or would you prefer them to be part of your supplier information management tool or sourcing suite in the future? Do you already have an integrated risk management (IRM) platform that could also address and support the type of supplier risk you are prioritizing? This will help guide your selection.

Evidence

2020 Gartner Future of Supply Chain Survey, n = 1,346 supply chain professionals. In September and October 2020, Gartner supply chain research sent invitations to complete an online survey to its community members, to Gartner clients, and to a wider group of practitioners in supply chain and other functions globally. We received 1,346 completed responses during the survey period. We had participants across industries — e.g., high tech (20%), healthcare and pharma (14%), consumer packaged goods (11%), industrial (10%), food and beverage (9%), and retail (9%). Most worked in supply-chain-related functions — e.g., supply chain (49%), logistics/transportation and distribution (9%), purchasing/procurement (9%), and operations (7%). Of the respondents, 57% were from North and South America, 29% were from EMEA, 13% were from Asia and Australia, and others were from the rest of the world. Additionally, 63% of participants were from companies with revenue of more than $10 billion, and 62% of participants were at VP/director level or above.

[1] **2021 Gartner Supply Chain Risk and Resilience Survey.** This survey was conducted to understand companies' current capabilities for supply chain risk management, where improvements are most needed, and where they are investing in processes, resources and technologies for the future. The research was conducted online 19 July through 3 September 2021, among 83 respondents in Germany and 6 in other countries. Gartner partnered with BME to recruit the participants. The sample was augmented with recruitment efforts through social media. Qualifying organizations operate in the manufacturing, healthcare, natural resources, retail, transportation and logistics, utilities, and wholesale trade industries. Qualified participants have a role tied to a supply chain function.

The survey was developed collaboratively by a team of Gartner analysts and BME leadership and was reviewed, tested and administered by Gartner's Research Data and Analytics team.

Disclaimer: Results of this study do not represent global findings or the market as a whole but reflect the sentiment of the respondents and companies surveyed.

[1] The Gartner supply chain research team conducted the **2021 Gartner Supply Chain Signature Series Risk Survey** to study the various approaches that supply chains take to mitigate risk. From August 2020 to March 2021, the research team conducted more than 70 interviews with CSCOs from large and midsize enterprises. Additionally, throughout December 2020, the research team sent out invitations to complete an online survey to a wide group of heads of supply chain globally. We received 262 completed responses during the survey period and analyzed the data, using a wide range of statistical procedures (e.g., simple t-tests, multiple regression analysis, and factor and cluster analyses).

[2] Supply Chain Brief: Risks of Growing Russian-Ukrainian Tensions Put Global Supply Chains on High Alert

[3] **2020 Gartner Supply Chain Disruption Management and Impact Survey.** This study was conducted to determine the types of disruptions that impact supply chains (positively or negatively), establish parameters that make a company fit or fragile when dealing with a disruption or turn, and identify the competitive and performance impact of supply chain disruptions. The research was conducted online from 31 March 2020 through 18 May 2020.

In total, 585 respondents were interviewed in their native language across North America (29%, n = 172; including the U.S. and Canada), Western Europe (39%, n = 225; including the U.K., Germany and Spain) and Asia/Pacific (32%, n = 188; including Australia, Singapore and China):

- Qualifying organizations operate in the manufacturing and retail industries and report anticipated enterprisewide annual revenue for FY20 of at least $250 million (at least $500 million in the U.S.).
- Qualified participants have a role tied to a supply chain function and are in director or above roles. All respondents are involved in their company's decisions regarding supply chain management processes, operations and strategies, either in a decision-making capacity or advisor to the decision makers.

The study was developed collaboratively by Gartner Analysts and the Primary Research Team.

Disclaimer: Results of this survey do not represent global findings or the market as a whole but reflect sentiment of the respondents and companies surveyed.

Note 1: Representative Vendor Selection

Although there are dozens more providers in the global supplier risk management market that often vary by geography, the vendors selected for this research represent one of the following:

- Solution providers that can deliver a global solution
- Market leaders in terms of size, revenue or market presence measured by marketing materials and Gartner end-user inquiries
- Solution providers that sell to enterprise-level companies

Note 2: Gartner's Initial Market Coverage

This Market Guide provides Gartner's initial coverage of the market and focuses on the market definition, rationale for the market and market dynamics.

Document Revision History

Market Guide for Supplier Risk Management Solutions - 17 November 2020

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Supply Chain Goes Full Tilt Into Risk Management

Procurement's Critical Role in Boosting Supply Chain Resilience

Manage Supplier Risk by Improving Supplier Visibility With Technology

Infographic: Supply Chain Visibility Is Fundamental to Resilience in Supply Ecosystems

Creating a Supply Chain Resilience Framework

Case Study: Resilient End-to-End Supply Chain Risk Management 4.0 Framework (HELLA)

Glossary of Risk Management Terms

Tool: Key Risk Indicators for Supplier Risk Management

4 Steps to Draft and Operationalize an Effective Supply Chain Risk Appetite Statement

Table 1: Supplier Risk Management Vendors by Area

Vendor	Event Monitoring	Financial	CSR	Performance	Compliance/ESG	Capacity	Cyber Risk
Achilles		X	X		X		X
apexanalytix	X	X	X	X	X		
Aravo	X			X	X		X
Coupa				X	X	X	X
Darkbeam							X
Dun & Bradstreet	X	X			X		
EcoVadis			X				
Elementum	X						
Everstream Analytics	X				X		X
HICX				X	X		
IntegrityNext			X		X		
Interos	X				X		X
Ivalua				X	X	X	

Vendor	Event Monitoring	Financial	CSR	Performance	Compliance/ESG	Capacity	Cyber Risk
JAGGAER				X	X	X	
Oracle				X	X		
NQC			X		X		X
RapidRatings		X					
Resilinc	X			X		X	X
riskmethods	X			X			X
SAP Ariba	X			X	X	X	
SupplierGATEWAY			X		X		
SupplyShift			X		X		
Zycus				X		X	

Source: Gartner (May 2022)

Table 2: Supplier Risk Management Vendors' General Information

Vendor	*Headquarters Location*
Achilles	Abingdon, U.K.
apexanalytix	Greensboro, North Carolina, U.S.
Aravo	San Francisco, California, U.S.
Coupa	San Mateo, California, U.S.
Darkbeam	Bristol, U.K.
Dun & Bradstreet	Short Hills, New Jersey, U.S.
EcoVadis	Paris, France
Everstream Analytics	San Marcos, California, U.S.
HICX	London, U.K.
IntegrityNext	Munich, Germany
Interos	Arlington, Virginia, U.S.
Ivalua	Redwood City, California, U.S.
JAGGAER	Morrisville, North Carolina, U.S.
Oracle	Austin, Texas, U.S.
NQC	Manchester, U.K.

Vendor	*Headquarters Location*
RapidRatings	New York, New York, U.S.
Resilinc	Milpitas, California, U.S.
riskmethods	Munich, Germany
SAP Ariba	Palo Alto, California, U.S.
SupplierGATEWAY	Santa Ana, California, U.S.
SupplyShift	Santa Cruz, Californiav
Zycus	Princeton, New Jersey, U.S.

Source: Gartner (May 2022)