

INSIGHTS FROM OUR 2024 SURVEY

# Risk Management in a Technology-Driven World



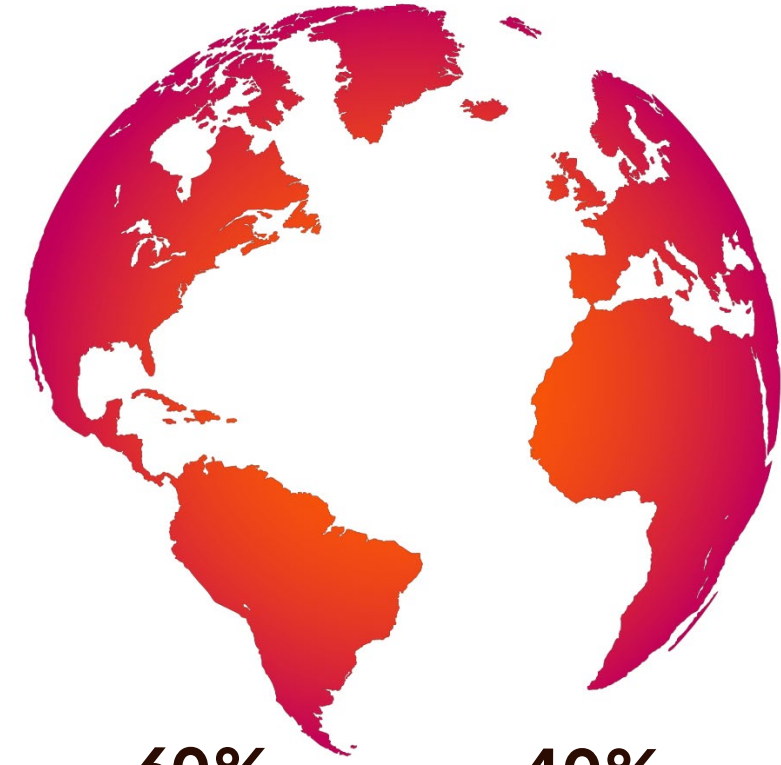


# 2024 Supply Wisdom

## Risk Management Survey

Over the course of two weeks from March 20 to April 2, 2024, we surveyed approximately **200 professionals** working in third party risk management, procurement, vendor management, and similar roles in the United States, Canada, United Kingdom, France, Germany, and Ireland.

**45% Procurement** **20% Other**  
**35% Supplier Management**



**60%** North America  
**40%** Europe

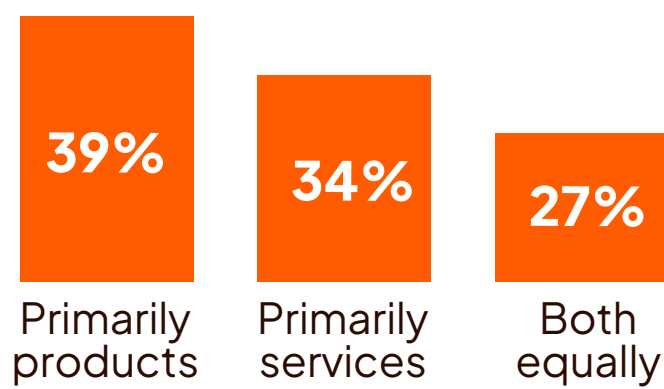
**50%** Manager

**34%** Individual Contributor

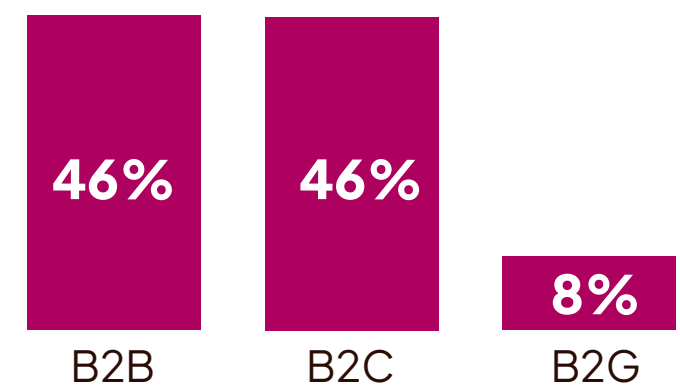
**12%** Director

**4%** VP/CXO (Chief Officer)

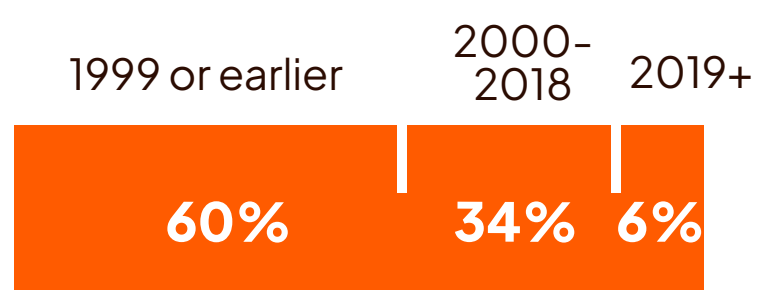
**Products/ Services:**



**Customer Source:**



**Company Founded in:**



**Company Headcount:**



Disclaimer: The terms "vendor" and "supplier" are used interchangeably in this document.

# EXECUTIVE SUMMARY

In today's fast-paced world of geopolitical, economic, and environmental uncertainties, there is no doubt that outsourcing non-core functions can save an organization time and money while also enhancing its ability to provide expanded products or services.

Executives are acutely aware of the cost savings – and the potential new revenues – that can exist from outsourcing, so the quicker new vendors can be onboarded, the quicker the financial and operational benefits can be realized. However, as boards and the C-suite pay increased attention to the geopolitical exposures of their business, the potential risks that may exist within their supply chains and vendor relationships have come into sharp focus.

Given the rapidly evolving business, technology, and political landscape in which we live and work inglobally, the primary objective of this survey was to learn about attitudes toward risk management practices at companies of varying sizes and locations. Specifically, we looked into how they are tackling risk assessment within their vendor and supplier populations, the types of risks they prioritize in their monitoring, their use of technology and artificial intelligence (AI) to monitor risk, and more.

The findings revealed several key themes:

**Most participants do not have a clear understanding of the make-up of their supplier, vendor, and contractor populations.**

**Differences exist between North American and European risk protocols, with European companies spending more time on vendor assessments yet North American companies feeling more confident in their protocols.**

**A disconnect exists between respondents' views on the importance of technology in risk management and their actual implementation of tools – namely AI – that could help them better understand their vendor population and monitor risks within it.**

**More than half of participants lack understanding of the risk levels that exist within their supplier populations. This creates a potential gap in the effectiveness of monitoring.**



## HIGHLIGHTS

At a high-level, the research found:

→ Despite over 50% of respondents not currently using AI in risk monitoring, more than half acknowledge the need to monitor for AI-related risks, indicating a growing awareness of technology's impact on risk management.

→ Nearly 80% of respondents view technology as very or extremely important in their risk management programs, yet there's a hesitancy to adopt the latest advancements, suggesting a disconnect between perception and action.

→ Only 14% of procurement and 13% of supplier management professionals report using continuous monitoring tools to assess suppliers, highlighting an underutilization of technology in risk assessment.

→ 62% of businesses don't strongly believe their risk monitoring program is meeting contractual and regulatory requirements.

→ North American (NA) companies use fewer third-party & Nth party vendors than European companies. 47% of European companies report vendors in as many as 49 countries, compared to 22% of NA companies who said the same.

→ The top risk-types monitored for are Financial Risk (65%), Operations Risk (64%), and Compliance Risk (51%) and Cyber Risk (51%).

This report dives into the survey's top findings with an eye toward providing you with practical insights to help strengthen your risk management approach and help protect your business.



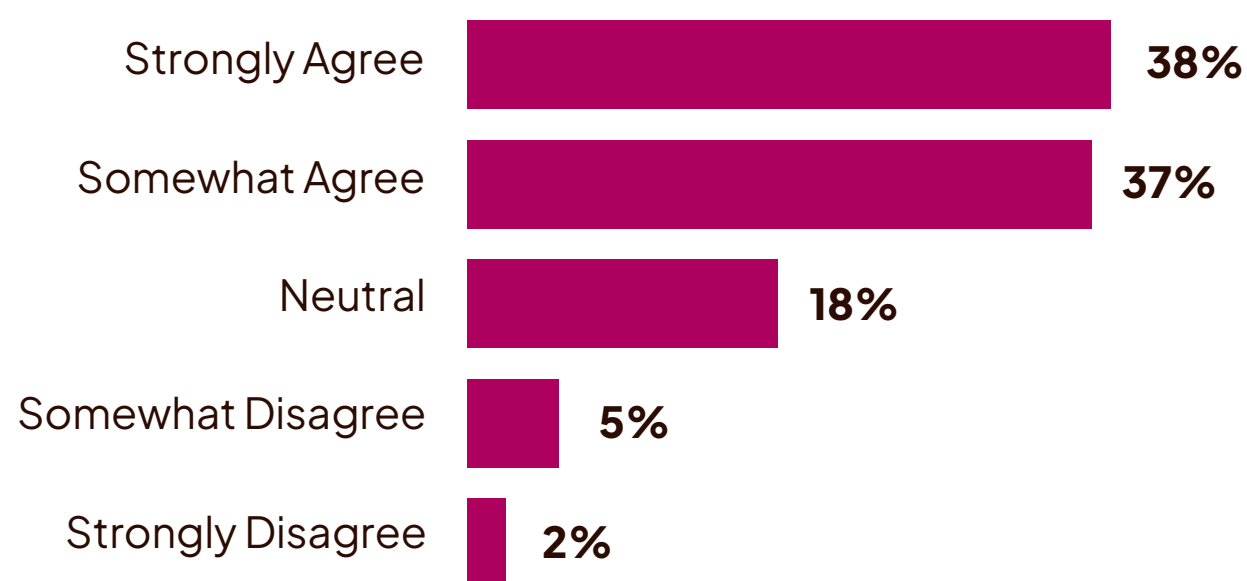
# Risk Assessment Protocols are Key, but...

## Lack of Confidence in Third-Party Risk Management is Concerning...

Vendor, supplier, and contractor assessment is key to a company's ability to truly know who they are doing business with. While 60% of the professionals surveyed said they assess vendors either monthly or quarterly and that they take up to a month to complete each assessment, they expressed a lack of confidence in the process, which is concerning.

### SURVEY QUESTION

Agree/Disagree: My organization's risk monitoring program is adequate in meeting and addressing company and regulatory requirements.



Base: 199 (99% of respondents)

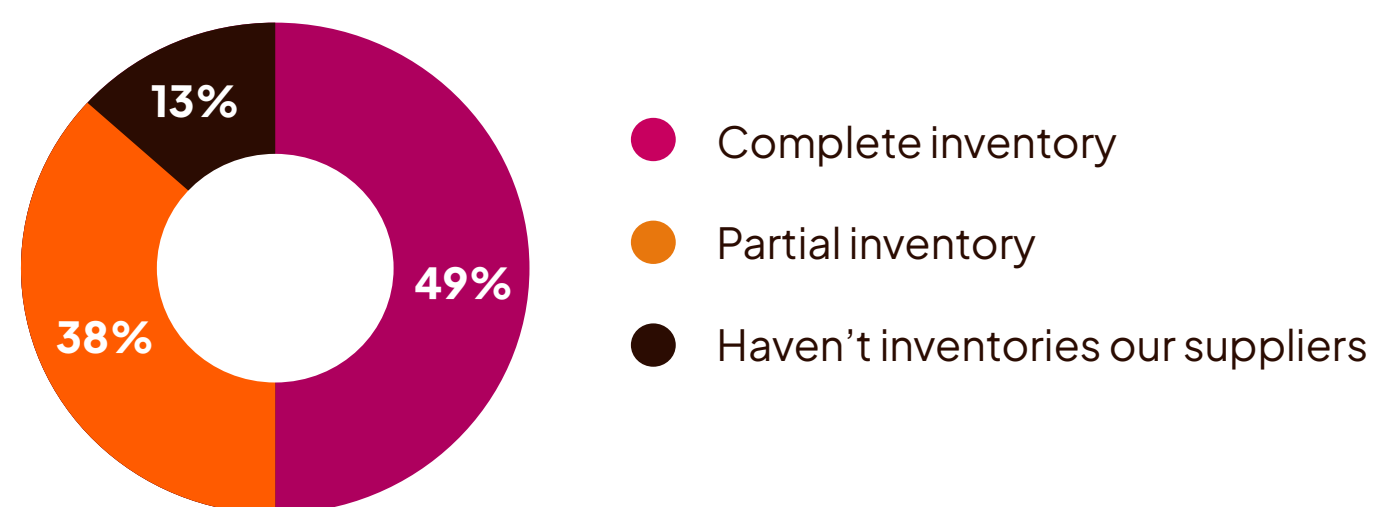
**62% of businesses don't strongly believe their risk monitoring program is meeting contractual and regulatory requirements.**

This may be attributed to the fact that...

**51% of participants report not having a complete supplier inventory list and 13% have no supplier inventory list at all.**

### SURVEY QUESTION

How would you characterize your organization's inventory of its supplier population?



Base: 142 (70% of respondents)

“

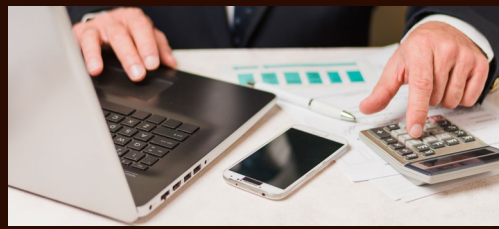
Conducting focused risk assessments that are based on current intelligence streamlines both the initial due diligence process and the lifecycle management process for companies. However, a company cannot adequately mitigate risks within their vendor populations if they do not even know who all of their vendors are.

- Jenna Wells, CTPRP

Chief Customer & Product Officer at Supply Wisdom

# HOW TO GAIN CONFIDENCE IN YOUR THIRD-PARTY RISK MANAGEMENT (TPRM)

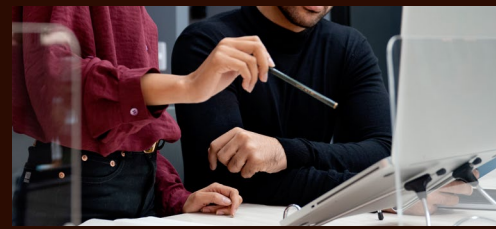
To begin remedying this, Supply Wisdom recommends:



Meeting with the **Accounts Payable team** to pull active spend reports for the last 12 months;



Meeting with the **Procurement team** to pull all active vendor contracts; and



Meeting with the **IT team** to learn which outside vendors have access to internal IT systems.

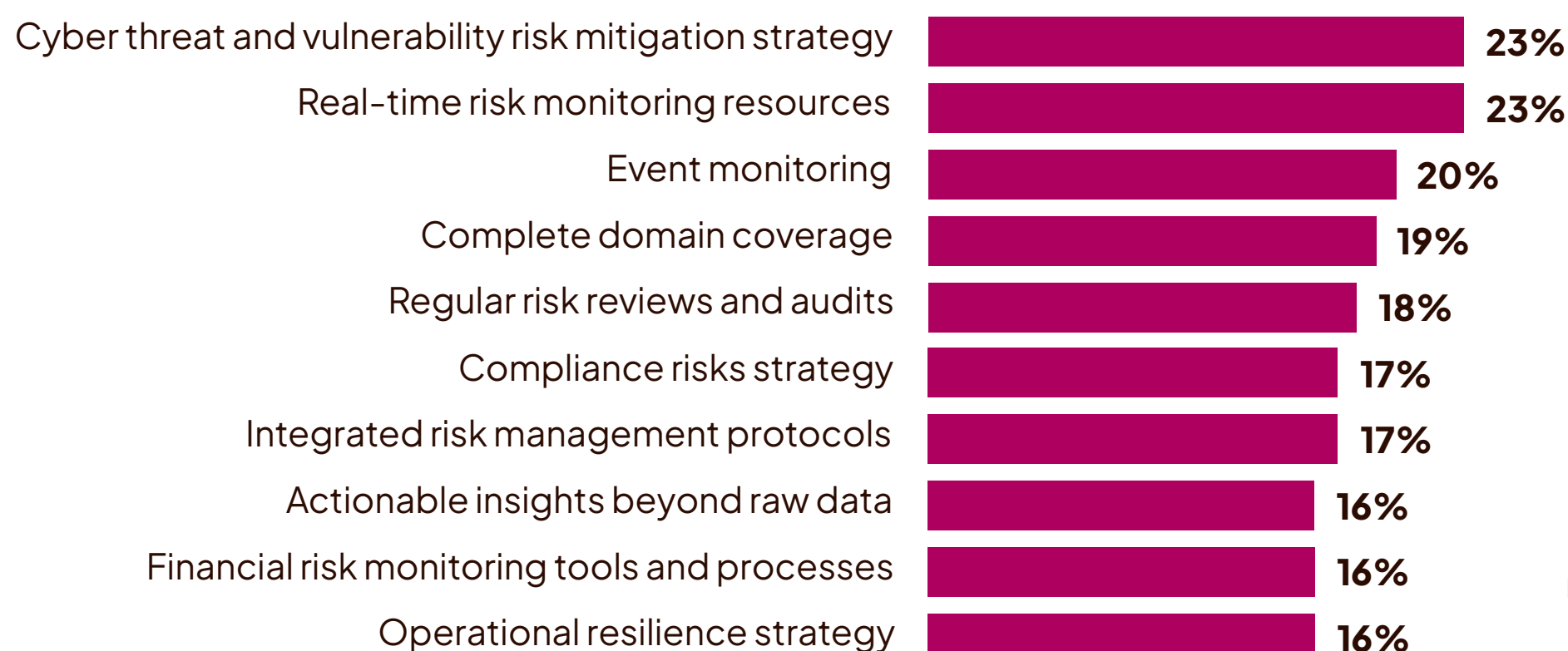


While **less than 15%** of both procurement professionals and their supplier management counterparts report using **continuous monitoring tools** to assess suppliers, interestingly, more than half (59%) of procurement professionals and nearly three-quarters (72%) of supplier management professionals said they use real-time continuous monitoring in their risk management processes. The second figure may be misleading as firms often believe they are leveraging continuous monitoring tactics by monitoring financial and cyber risks, but they are not actually leveraging automation to enhance detective controls across the broad landscape of risk types capable of causing a business disruption, and which are raise the minimum expectation of regulators.

“ Unlike point-in-time risk assessment, continuous monitoring provides strategic insight into a third-party. For example, it is more important to understand scenarios such as whether a third-party has lost key clients recently, is experiencing liquidity and debt service issues, has failed to restructure its debt and has had to sell business units to raise capital or has been partially nationalized by the host government, and is at increased risk of a ransomware attack than whether it has an already completed questionnaire, ” said Hannah Ford, CTPRP, Head of Product at Supply Wisdom.

## SURVEY QUESTION

What do you feel is lacking from your company’s current risk monitoring program?



Base: 152 (75% of respondents)  
Note: Respondents could select multiple options. Showing only the top 10 most selected options.

# Artificial Intelligence is Here to Stay

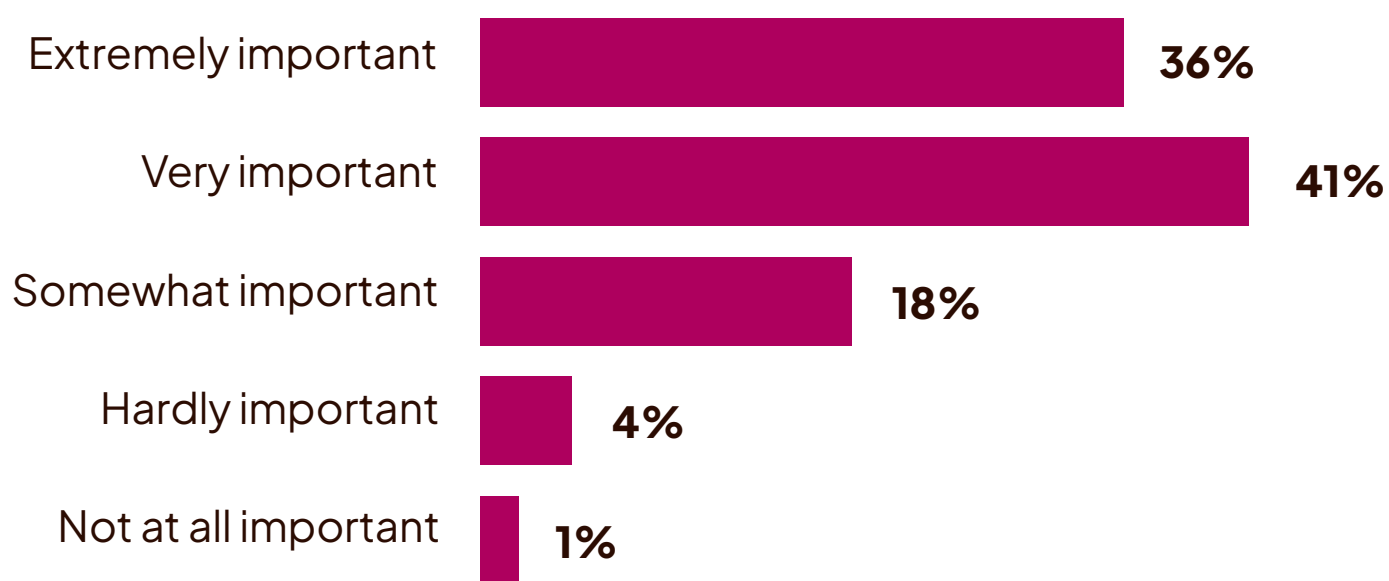
The emergence of AI has taken the world by storm, raising eyebrows about its impact on businesses and creating a swirl of negativity about the associated risks. While there are important risks that need to be considered by regulators, companies, and creators, there are important positives that cannot be overlooked.

“ Given that AI can learn from humans, it can be a very powerful tool to help make roles easier and create operational efficiencies for companies. In fact, disruption avoidance through forecasting and predictive analytics allows risk management to further support revenue growth, ” said Madhuri Karnam, Research Analyst at Supply Wisdom. “The emergence of AI in the risk domain highlights the importance of knowing who you are doing business with from a supplier, vendor, and contractor perspective. The bottom line is that AI is here to stay, so businesses need to figure out how to mitigate its risk and navigate its use.”

As mentioned earlier, there appears to be a disconnect between respondents’ views on the importance of technology and their implementation of the latest tools. While nearly 80% say technology is very important or important to risk management, 57% say they are not using AI in their risk assessment program.

## SURVEY QUESTION

How important is technology to your organization’s risk management program?

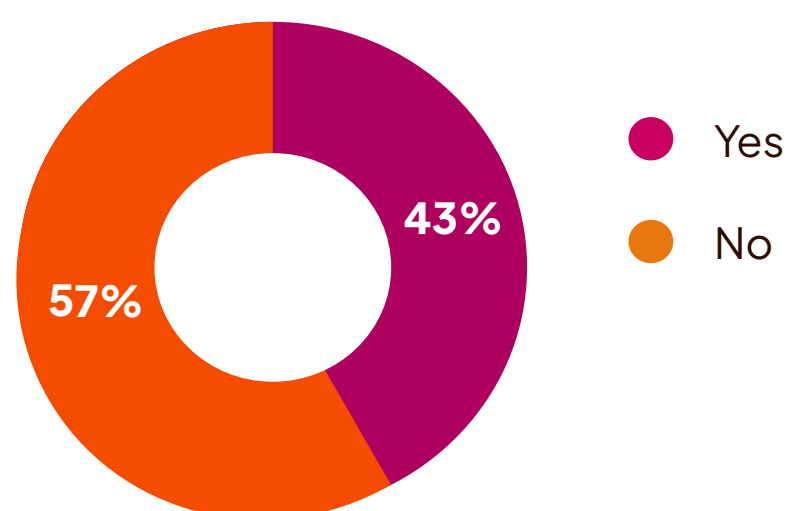


Base: 202 (All respondents)

**Nearly 80% agree – technology is important in their TPRM, yet there's a hesitancy to adopt the latest advancements, suggesting a disconnect between perception and action.**

## SURVEY QUESTION

Is your organization using AI/ML or generative AI tools in your current risk assessment process?



Base: 166 (82% of respondents)

**Despite this, more than half acknowledge the need to track and investigate AI related risks within their supplier populations.**



# Differences Exist Between

## European and North American Risk Protocol

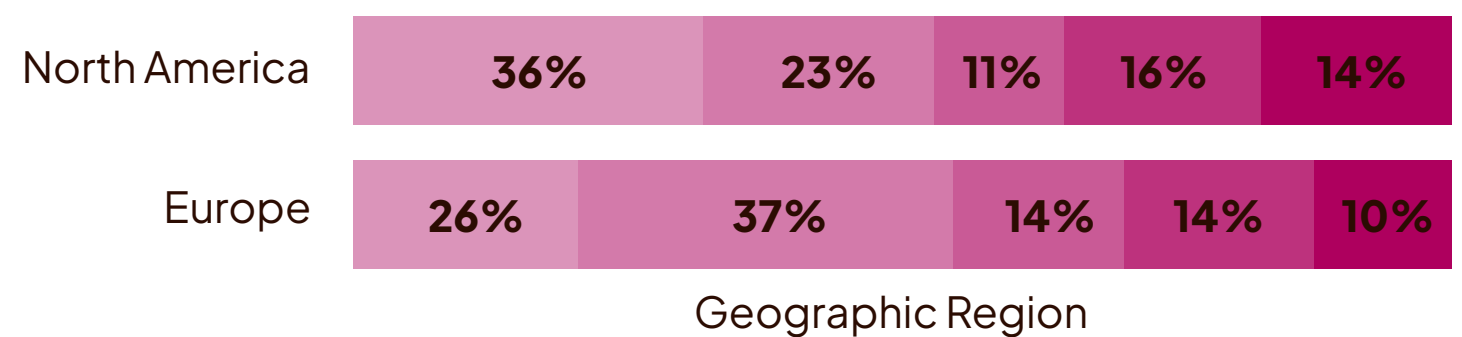
European companies appear to spend more time on vendor assessment than their North American counterparts, but interestingly, North American respondents appear to feel more confident in their risk management protocols and may be in a better position to manage risks.

Indeed, **North American companies are more likely to assess vendors monthly** than European companies (36% vs. 26%) whereas **European companies prefer quarterly assessment** (37% vs. 23%) and spend more time per assessment, with 35% spending 5-6 weeks per assessment, compared to only 18% of North American companies.

### SURVEY QUESTION

**How frequently are your organization's suppliers/vendors assessed?**

- Monthly
- Quarterly
- Semi-Annually
- Annually
- Continually - We use continuous risk monitoring

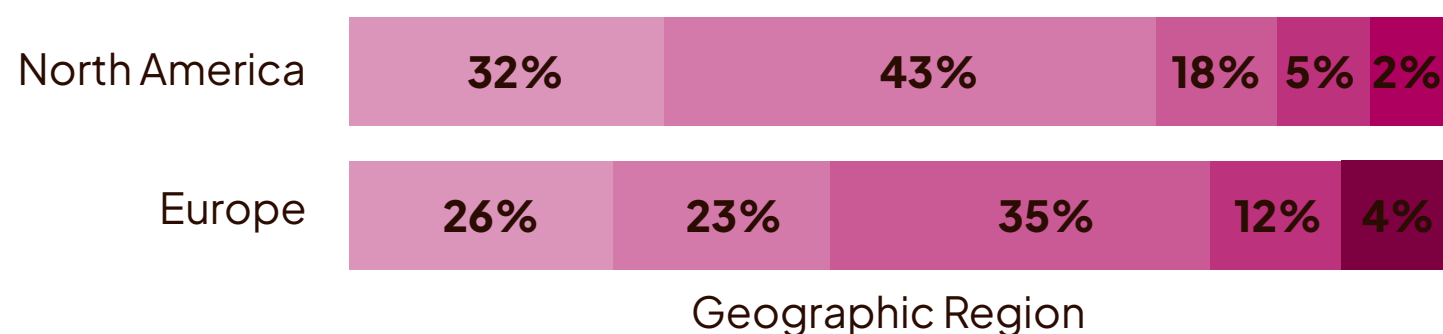


Base: 187 (93% of respondents)

### SURVEY QUESTION

**In how many geographic locations are your third-party and Nth party suppliers and partners located?**

- 1 country
- 2-4 countries
- 5-19 countries
- 20-49 countries
- 50-99 countries
- 100+ countries



Base: 183 (91% of respondents)

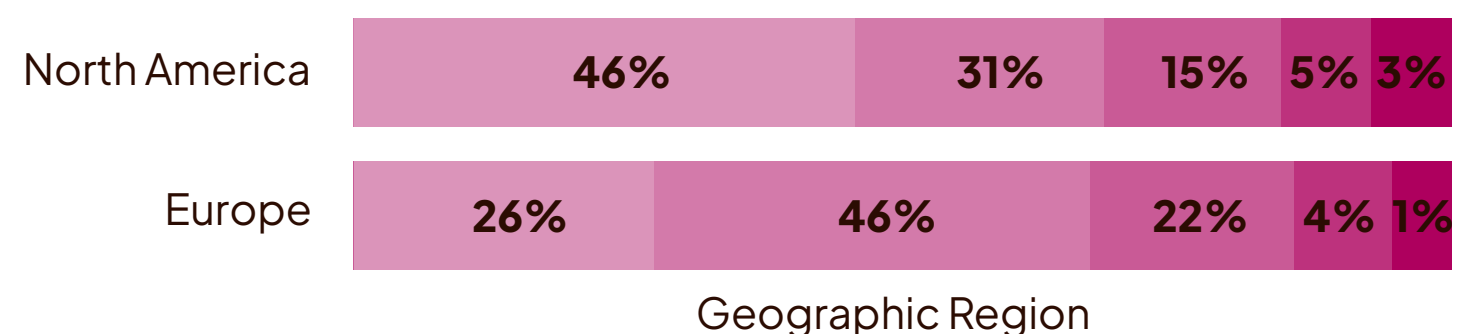
**North American companies also use fewer third and Nth party vendors in fewer locations** than their European counterparts. In fact, 75% of North American companies reported vendors in four or fewer countries, while only 49% of European respondents said the same; with 47% of European companies reporting vendors in as many as 49 countries, compared to 22% of North American countries who said the same.

Perhaps unsurprisingly, less than half (**46%**) of North American companies strongly agree that their risk management program is adequate at meeting or addressing company and regulatory requirements, compared to only **26%** of European companies.

### SURVEY QUESTION

**Agree/Disagree: My organization's risk monitoring program is adequate in meeting and addressing company and regulatory requirements.**

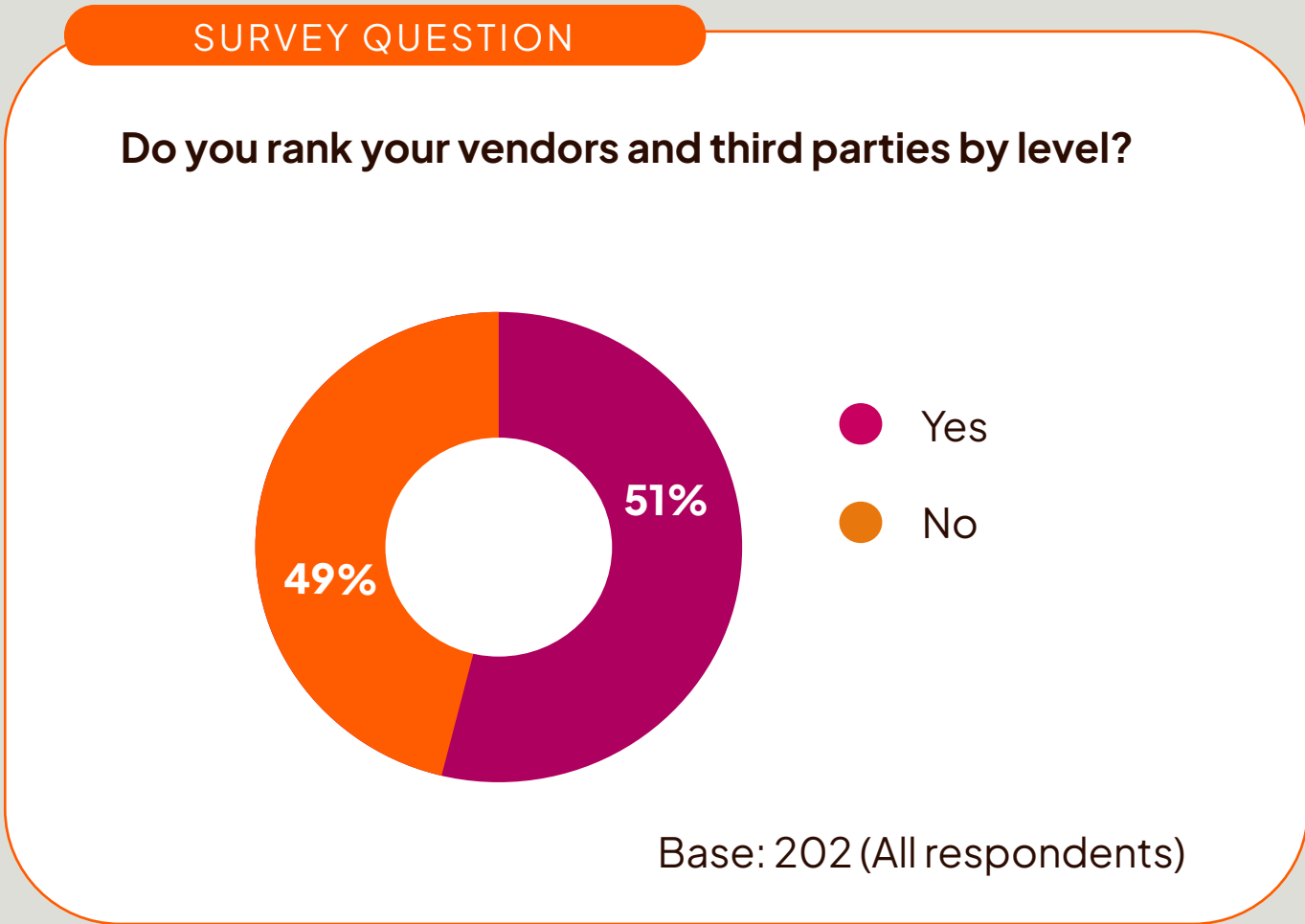
- Strongly agree
- Somewhat agree
- Neutral
- Somewhat disagree
- Strongly disagree



Base: 199 (99% of respondents)


# Third-Party RED FLAGS

In addition to not having a complete view of vendors and suppliers, not understanding the levels of risk that exist within supplier populations can be another gap in the effectiveness of a monitoring program. **Nearly 50% of the companies surveyed do not rank their vendors and third-party providers by risk level at all.**



## Ranking Vendors is Uncommon.

This creates inefficiencies for already understaffed teams who could benefit from knowing where to focus their assessment or continuous monitoring efforts. Many global regulations and contractual obligations require certain monitoring and reporting standards, which cannot be achieved without first knowing where the risk lies within a vendor population. It is also important to keep in mind that not all vendors are created equal – some have access to sensitive data, provide services in volatile locations, and can be critical to ensuring a business stays operational. Determining both the Inherent and Residual Risk within the vendor population of an organization affords the opportunity to adequately monitor these vendors on a continuous basis to ensure compliance and smooth operations.



Failure to rank vendors can lead to:

- ➔ Siloed view of the vendor population and an inability to determine (or comply with) company risk appetite statement/risk tolerance;
- ➔ Inability to adhere to contractual and regulatory requirements;
- ➔ Reactive Risk Management if/when an event does occur affecting a third-party, leading to a lack of understanding around the criticality of the vendor to the company and whether it has access to sensitive data.

“ Given the state of play in geopolitics, ongoing wars and global conflicts, environmental issues, and more facing the world, companies are recognizing the need to proactively assess and mitigate location-based risks to ensure business continuity and resiliency. The need for location-based monitoring cannot be understated, and as such third-party risk always needs to be tied to location risk. This means it is critical to know and monitor the locations where your third-party providers are operating from – not just the location of their headquarters – in addition to monitoring the risks associated with your own location. ”

– Victor Meyer  
Chief Strategy Officer at Supply Wisdom



# Third-Party RED FLAGS

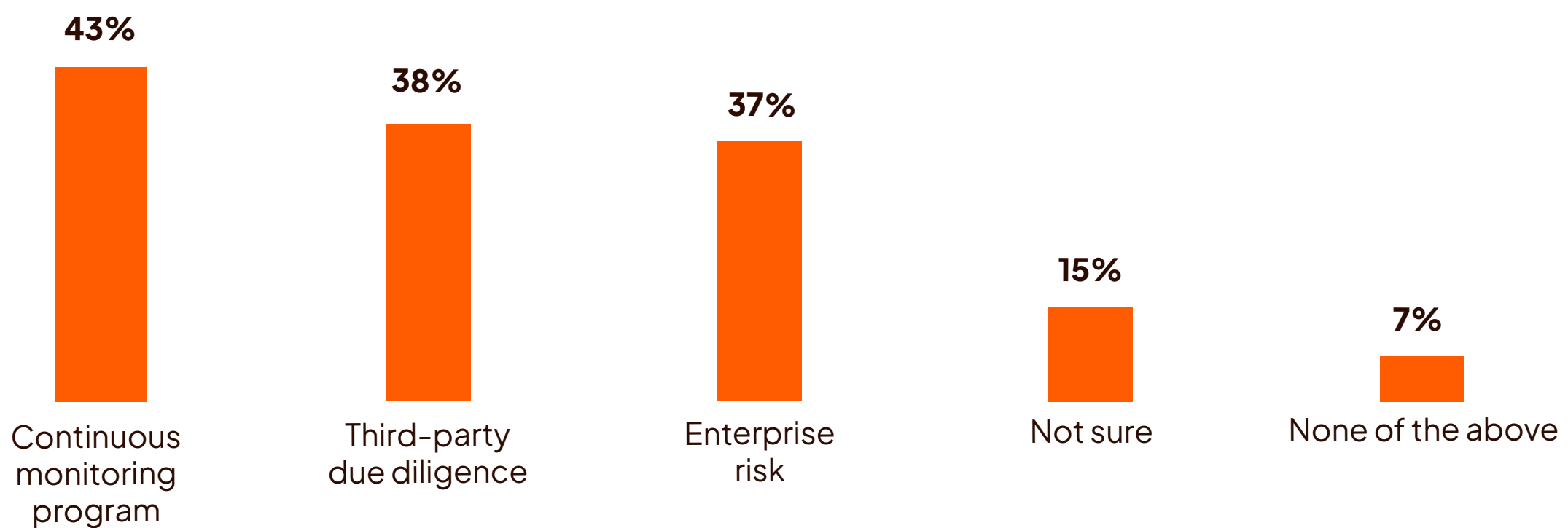
## Location Risk is Overlooked.

In fact, more than half of respondents said they are not monitoring location at all. This puts companies at risk because compliance failure is imminent, and there is an innate inability to react quickly to unplanned events – such as the recent Francis Scott Key Bridge collapse in Baltimore or the Taiwan earthquake. Companies with strong location monitoring will ultimately surpass those without it.



### SURVEY QUESTION

Have you operationalized location risk into your third-party risk model?

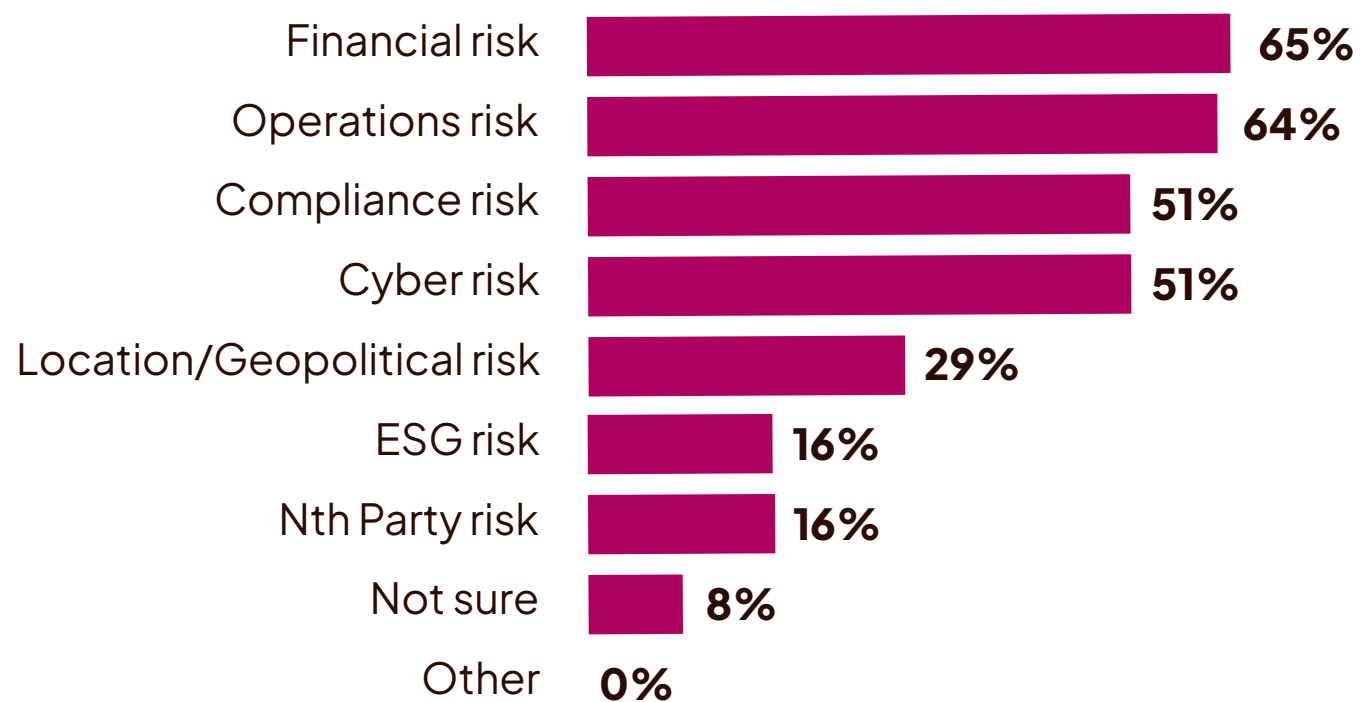


Base: 202 (All respondents)

Note: Respondents could select multiple options.

### SURVEY QUESTION

For which types of risk is your organization monitoring?



Base: 202(All respondents)

Note: Respondents could select multiple options.

## Financial risk is still a top priority for companies.

According to the data, businesses prioritize financial risk over other risks. The top risk-types monitored for are Financial Risk (65%), Operations Risk (64%), and Compliance Risk (51%) and Cyber Risk (51%). Interestingly, only 29% said that Location / Geopolitical Risk is a priority, while even fewer (16%) are making ESG Risk a priority. This is of concern on several levels given the uncertainties that exist in many parts of the world currently and the volume of natural disasters that continue to occur, both of which have the capacity to massively impact the supply chain and business generally.

# Strategies for an Evolving Risk Environment

We live in an increasingly **volatile and unpredictable world**, where the pace of change is more rapid than ever before. Companies, driven by the need to stay competitive while reducing costs, are outsourcing various functions to third-parties with increasing frequency. The trend shows no sign of slowing as businesses seek specialized expertise and efficiencies, but this extensive reliance on third-party vendors brings a host of new challenges and risks.

**Contractual requirements** have become more stringent, demanding higher levels of compliance and accountability. At the same time, the **regulatory environment** is growing more complex, with new laws and guidelines continuously being introduced, necessitating constant vigilance and adaptation. **Disruptions**, whether due to geopolitical instability, economic fluctuations, or technological failures, are inevitable and can have far-reaching impacts.

To proactively manage these multifaceted risks, it is crucial for companies to have an accurate and **holistic view** of their third-party population. This involves not only identifying all third parties but also tiering them by criticality, ensuring that those who have the most significant operational impact are closely scrutinized. Additionally, **tagging these third parties** to specific locations can help in understanding and mitigating **geographic risks**, while **continuous monitoring** is essential to keep track of their performance and any emerging issues that could affect the company.

**To stay ahead of the competition**, it is vital to focus on these areas when building risk management programs from the ground up. Doing so helps to create a resilient framework that not only safeguards an organization against potential threats but also enables it to thrive in an ever-changing landscape. While this requires a strategic approach that integrates advanced technologies and analytics to provide real-time insights and facilitate informed decision-making, taking a proactive stance will help ensure that a company remains agile and responsive to both current and future challenges.



**Be innovative. Rethink Risk. Unlock Revenue.**

To learn more about this survey or get in touch with our team, contact us at [info@supplywisdom.com](mailto:info@supplywisdom.com)

[www.supplywisdom.com](http://www.supplywisdom.com)