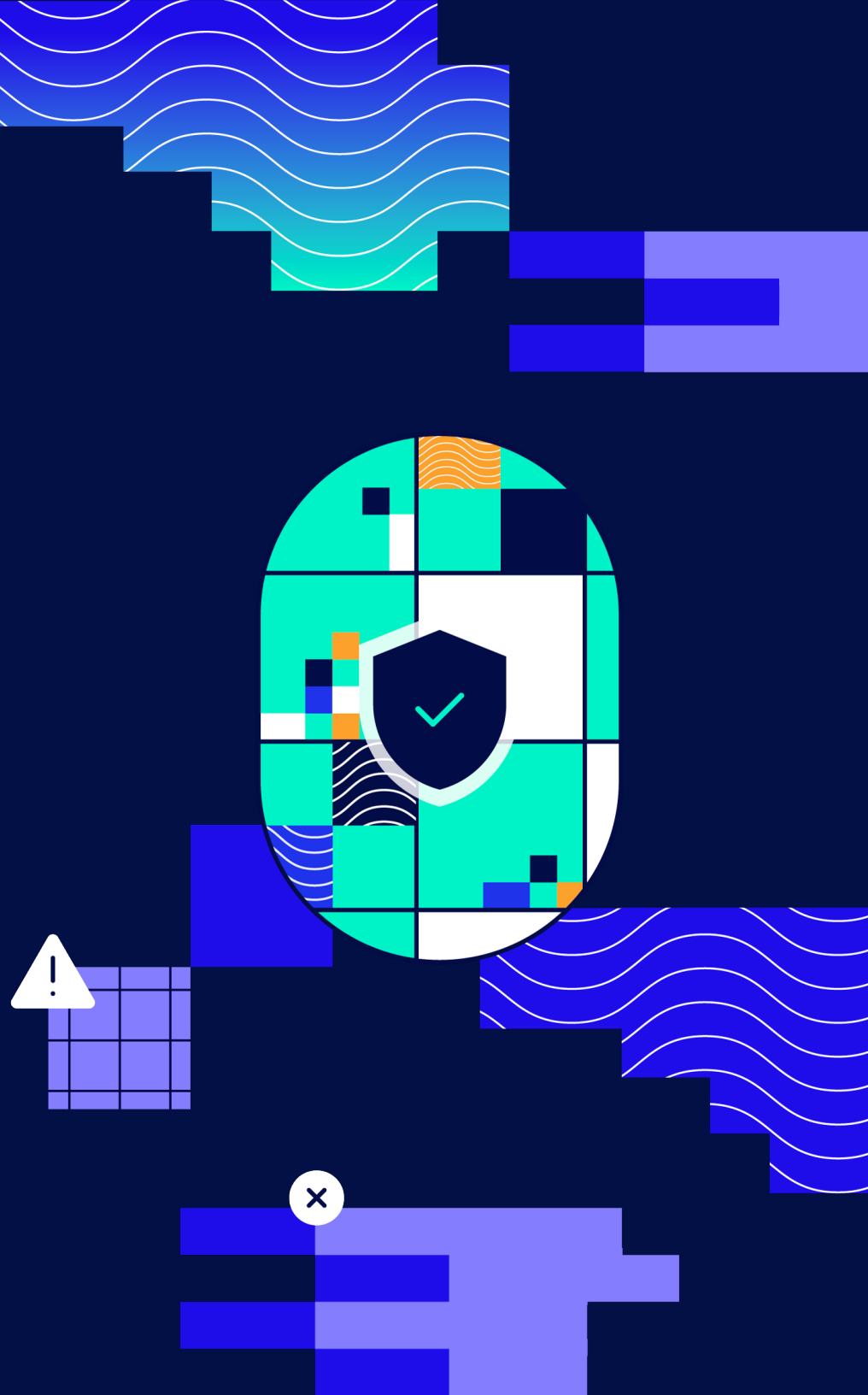
interos

THE THIRD ANNUAL INTEROS SUPPLY CHAIN SURVEY

Invisible Threats: Resilience 2023



interos.ai

Table of Contents

Foreword

“Supply chain resilience is more than just a response to disruptions; it’s an active pursuit of change through a blueprint known as Resilience by Design™. As organizations continue to wrestle with multiple risks associated with climate change, geopolitical turmoil, rising sanctions and controls, inflation, and financial instability, our annual survey demonstrates an urgent need for a more rigorous and anticipatory approach to risk detection and mitigation through leading vs lagging indications.

With the right people, processes and technology, Supply chain risk management (SCRM) and third-party risk management (TPRM) can evolve from mere compliance into an engine for long-term value creation by driving brand value, reputation and profitability.

In a world where swift adaptation is key to performance, AI technologies and a designed approach to resilience enables leaders to act five days sooner, think five moves ahead, and see five layers deeper.

Collaboration is paramount too, both internally and externally. While procurement naturally manages supplier risk, other functions play crucial roles. Managing a global risk network demands open communication, joint initiatives, and sometimes, shared investments with suppliers. Crucially, it also demands shared intelligence – made accessible through common-use technologies that continuously surface essential insights and reduce background noise.

Resilience by Design™ is only achievable through a willingness to leave behind strategies that no longer work. By prioritizing visibility, proactive risk navigation, and sustainability, we can ensure that today’s complex and fast-moving enterprises remain unstoppable.”

JENNIFER BISCEGLIE,
Interos Founder & CEO

Overview

Welcome to Resilience 2023, Interos' annual survey of global supply chain leaders.

This year, we surveyed hundreds of senior supply chain decision makers across aerospace & defense, financial services, energy, healthcare, and government to understand how changing industry dynamics are playing out across multiple sectors, bringing new insights, trends, and best practices for procurement professionals.

While the overall cost of disruption has waned in the post-pandemic era, a new wave of regulatory action – and the desire to deliver improved customer experiences while protecting brand reputation – is driving organizations to advance their SCRM/TPRM maturity.

Read on to learn more about how operational resilience has become a defining competitive differentiator.

Key Findings

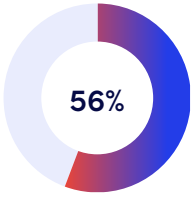
4

The average organization suffers **four supply chain disruptions** requiring significant mitigating action annually

↑ $37M

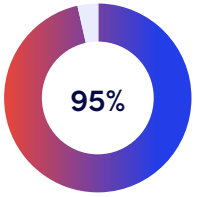
Organizations believe they **could gain $37M annually** by preparing better for and reacting faster to disruption

RISK ASSESSMENT



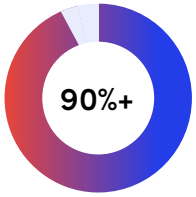
On average, organizations only assess 56% of their critical suppliers for risk

RISK MANAGEMENT MATURITY



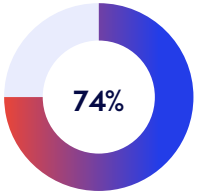
95% of organizations do not consider themselves to have reached the uppermost stage of SCRM/TPRM maturity

EVENT AWARENESS



90%+ of organizations would not be aware of a supplier disruption in all the tiers of their supply chain within **48 hours of occurrence** (varies by type of disruption)

DATA, ANALYTICS AND SOFTWARE



74% of procurement leaders agree that they cannot hope to comply with emerging regulations without supporting data, analytics, and risk management software

Out of the

750

Senior procurement leaders we surveyed...

400 are from the **United States**

200 are from the **UK and Ireland**

150 are from **Canada**

= 10 individuals

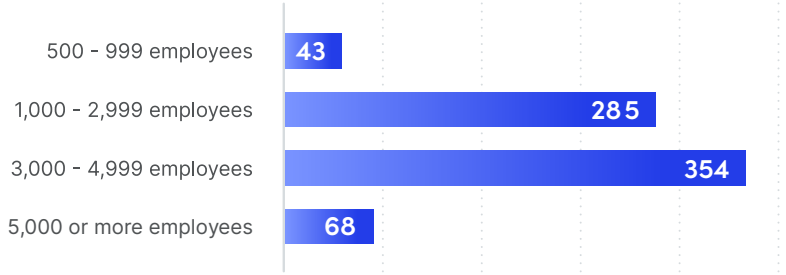
319 are within senior management

431 are C-level or board members

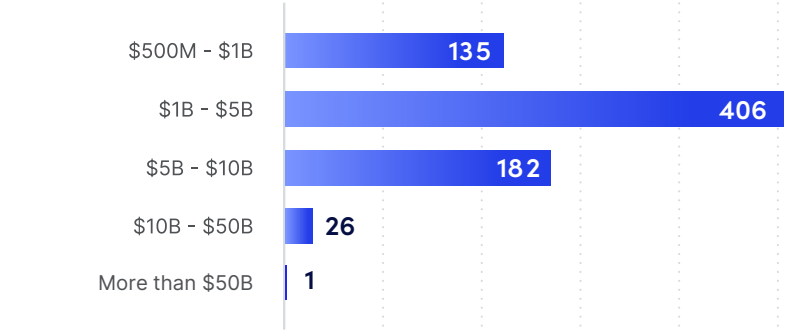
Demographics

750 senior procurement decision makers were surveyed in April and May 2023, split in the following ways:

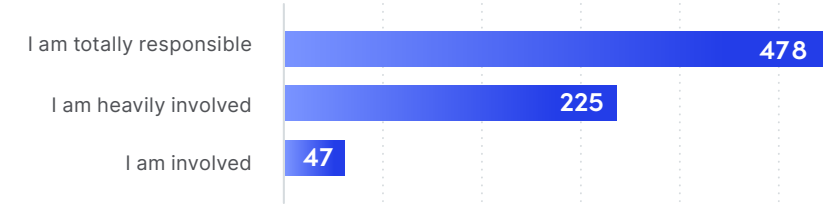
Q: How many employees does your organization have globally?



Q: What is your organization's global revenue in USD?



Q: What is your level of involvement when it comes to managing the global supply chain in your organization?



Q: Within which sector is your organization?

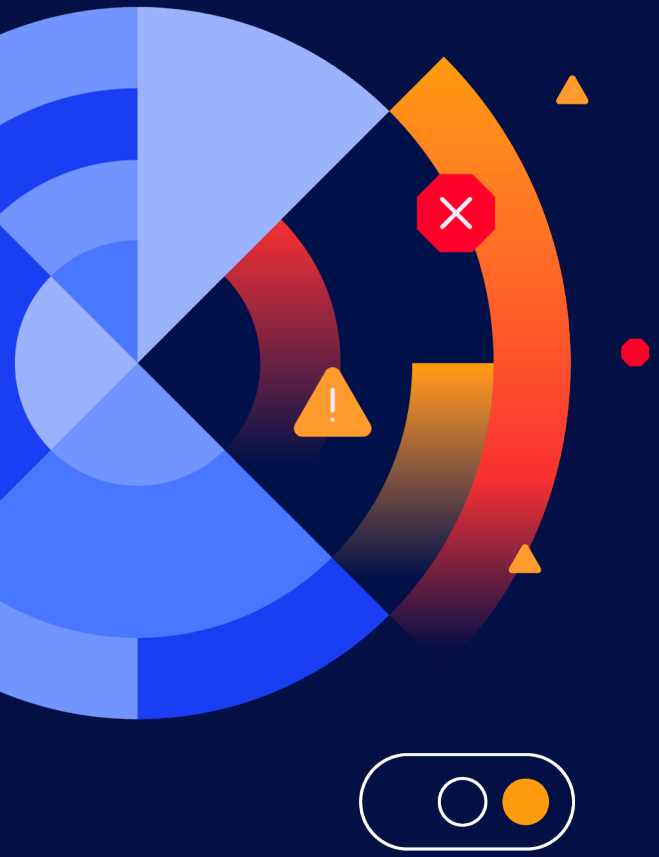
150

individuals each are from the following industries:

- Energy, oil/gas and utilities
- Financial services
- Healthcare (private and public)
- Federal/national/ central government
- Aerospace and defense

SECTION 01

A World of Supply Chain Disruption



Impact of Supply Chain Disruptions and Top Risk Concerns in 2023-24

The havoc wrought by the COVID-19 pandemic may have subsided during the past year, but plenty of other disruptive events continue to impact organizations and their supply chains in 2023. They include:

- Russia's brutal and unprovoked war in Ukraine
- Rising geopolitical tensions between the United States and its allies and China, including the threat posed to semiconductor powerhouse Taiwan
- Sanctions, export controls and other restrictions on Russian and Chinese entities, including those centered on the supply of advanced technologies
- Cost inflation in energy, food and a wide range of commodities and services
- A steady stream of cyber attacks, data breaches and ransomware demands by malign state actors and criminal groups
- Bank collapses in the U.S. and Europe, and concerns about the stability of the global financial system and possible recession
- Wildfires, flooding, drought, earthquakes and other catastrophic natural disasters

Supply Chain Disruptions Are Frequent and Costly

On average, the 750 organizations in financial services, aerospace & defense, healthcare, energy and central government that participated in our study reported having to deal with four major supply chain disruptions during the past 12 months. These were events that required significant mitigating action – for example, switching suppliers and/or locations, rerouting logistics, delaying customer orders, and so on.

The annual financial impact of these disruptions, in terms of lost revenue and additional costs, is also significant. While lower than the figure reported in our 2022 study, the mean average of $82 million among organizations with at least $500 million in annual revenue remains a material sum – one that most procurement leaders surveyed are keen to reduce.

> "At a global level we haven't done a good job managing risk. We assumed everything would work flawlessly. And now we know it doesn't."
>
> **– Procurement Leader,** Energy & Utilities, U.S.

4 **UP 33%**
FROM 2022

Number of supply chain disruptions that required organizations to take significant mitigating actions in the past 12 months

$82M

Annual financial impact as a result of these supply chain disruptions

$22M

The estimated average cost per disruption.*

* When estimating these costs, respondents selected from cost ranges, and for the purposes of our calculations, Interos used the midpoint of those ranges. Thus, the specific cost-per-significant disruption should be considered a very broad estimate and real disruption costs will vary widely based on factors unique to companies and their supply chains

$111M

Average annual cost of disruption for companies with $10B – $50B in annual revenue

$43M

Average annual cost of disruption for companies with $500M - $1B in annual revenue

Costs by Vertical (in USD millions)

Among our survey findings, financial services, energy, and healthcare suffered significantly greater financial losses due to supply chain disruption than organizations in aerospace & defense or government.

This disparity could be attributed to the fact financial services, energy, and healthcare sectors are often immediately and heavily reliant on global networks for their operation. For instance, financial services rely heavily on complex, interconnected global systems for data processing and transaction execution.

Conversely, aerospace & defense, and government sectors often have more controlled, localized supply chains, with contingencies and stockpiles in place due to the criticality of their work. These sectors are also less demand-sensitive, with demand being driven more by long-term contracts and government policies, rather than immediate consumer needs. They may have more buffers in place to absorb and manage supply chain disruptions, hence experiencing less financial loss when such disruptions occur. It is worth nothing that A&D organizations consistently ranked themselves as the most-mature of the industries surveyed.

Larger organizations also, naturally, incurred greater costs – though those costs did not scale 1:1 with revenue. On average, companies with between $500 million and $1 billion in annual revenue incurred costs of $43 million, whereas for firms with $10-50 billion in revenue the comparable figure was $111 million.

> “We have to recognize that there is risk, things cost money, and if we keep using the lowest cost provider model - we’ll keep painting ourselves into corners. I’m irritated about it to say the least.”
>
> – **Procurement Leader,** Energy & Utilities, U.S.

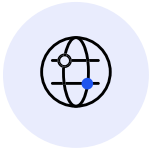
Q: What annual cost increases and/or revenue losses does your organization experience annually?

FINANCIAL

$44M

CATASTROPHIC

$45M



GEOPOLITICAL

$45M

CYBER

$43M

ESG

$44M

RESTRICTIONS

$47M

Six Major Categories of Supply Chain Risk

Within this overall financial impact, executives reported annual cost increases and/or revenue losses ranging from $43 million to $47 million in each of six distinct risk categories:

- **Financial**, including supplier health and insolvency
- **Catastrophic,** including extreme weather, natural disasters and factory fires
- **Geopolitical**, including wars, terrorist attacks and global trade disputes
- **Cyber**, including data breaches, ransomware demands and attacks on critical physical and digital infrastructure
- **ESG,** including environmental factors such as carbon emissions and pollution, plus social factors such as forced and child labor
- **Restrictions**, including sanctions and export controls imposed on named entities, individuals, and technologies

This latter category, which has seen a big increase in use by Western governments aimed at Russian and Chinese targets in particular during the past year, was the most expensive. But the findings highlight that organizations cannot afford to disregard any type of supply chain or third-party risk if they wish to minimize the financial impact of disruptive events.

> "The magnitude of supply chain risk is higher than ever before. We created a supply chain risk map to identify potential risks, their likelihood and the potential consequences to us."
>
> – **Procurement Leader,** Aerospace & Defense, U.S.

"Scarcity of essential raw materials, components and supplies is coming from across the world, with prices higher than ever before. Add in the Ukraine war and we are in the most vulnerable supply position that I can remember."

– Procurement Leader,
Aerospace & Defense, U.S.

45%

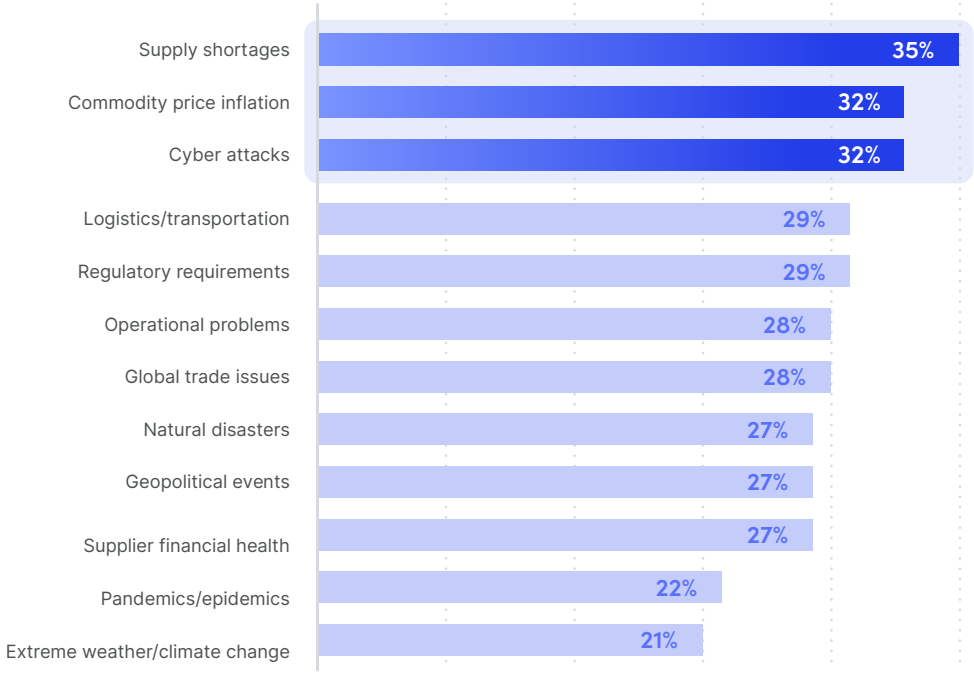
of A&D firms put cyber attacks in their top 5 risks

Top Risks: Supply Shortages, Inflation, Cyber Attacks

The types of risk that procurement leaders are most concerned about reflect the current global environment, with supply shortages and inflation topping the list. Worries about supply shortages – a COVID-19 legacy exacerbated by the Ukraine war – are especially high in the energy and government sectors. Almost half of A&D firms (45%) are concerned about the other leading risk – cyber attacks – which, aside from being an operational, reputational and financial security risk, have become a common component of "conventional" wars over the last decade.

Only in healthcare is the threat of further pandemics or epidemics a top concern, with one-third of respondents listing this vulnerability among their top five, compared with just 22% of the sample overall.

Q: Which of the following types of supply chain risks are you most concerned about in your organization during the next 12 months? (Top 5 risks)



	Regulation	Impact*
	Uyghur Forced Labor Prevention Act (UFLPA)	72%
	National Defense Authorization Act (NDAA) Section 889	72%
	Interagency Guidance on Third-Party Relationships – US	70%
	Digital Operational Resilience Act (DORA)	65%
	Corporate Sustainability Due Diligence Directive (CSDDD)	66%
	Critical Raw Materials Act – EU (proposed)	64%
	OSFI B-10 TPRM Guideline	66%
	German Supply Chain Due Diligence Act	61%
	PRA/FCA Operational Resilience Regulations	67%

* Significant or moderate impact

Supply Chain Legislation Will Have a Material Impact

Regulatory requirements are another top-rated risk for 2023-24. The past year has seen the introduction of several laws on both sides of the Atlantic that specifically target supply chain or third-party risk – notably in the realms of ESG, cybersecurity and operational resilience – with a slew of others in the pipeline.

The U.S. Uyghur Forced Labor Prevention Act (UFLPA), which came into effect in June 2022, gives border officials powers to seize shipments of products suspected of being made using forced labor in the Xinjiang region of China. More than 4,600 shipments worth in excess of $1.6 billion have been detained so far, according to the U.S. government. No wonder almost three-quarters of procurement leaders (and 80% in the U.S.) consider the UFLPA will have a "significant" or "moderate" impact on their organizations.

Tightening rules around the sourcing of Chinese technology in U.S. federal government contracts (Section 889 and 5949) are similarly high profile, while in financial services, proposed new rules in the U.K., Canada, the U.S. and the European Union – including the Digital Operational Resilience Act (DORA) – are regarded as impactful by approximately two-thirds of survey respondents.

Not all impact is negative, however. Indeed, the majority of CPOs consider legislation helpful in forcing their organizations to improve supply chain and third-party risk management capabilities, as described in the next section.

Shortages, Costs, Protectionism Are Top Concerns

Geopolitical tensions are another source of concern. Although a moderate risk in the overall ranking for the coming year, the crisis in Ukraine and the ramping up of U.S.-China rhetoric around decoupling, economic coercion, espionage and Taiwan's independence, among other issues, has forced geopolitical risk higher on the executive agenda.

When asked specifically about the potential impact of geopolitical tensions on their suppliers and supply chains over the next three years, 85% of survey participants say they are "extremely" or "somewhat" concerned.

Considering the specific impacts of geopolitical risk, supply shortages and additional costs are uppermost in CPOs' minds. They are also concerned about how government industrial and national security policies are reshaping global trade in a more protectionist direction, and about the increased threat to critical infrastructure (ports, power plants, internet connectivity and the like) from military or cyber attacks.

These concerns are closely balanced against the potential costs of some resilience-building measures. These include the costs of establishing new suppliers or manufacturing facilities, higher inventory carrying costs, and the costs of maintaining redundant systems or processes. As companies strive to be more resilient in the face of growing threats, they must also grapple with the challenge of efficient implementation.

As we'll see later in the report, increasing supply chain visibility may be the missing piece leaders need to help make these investments efficiently.

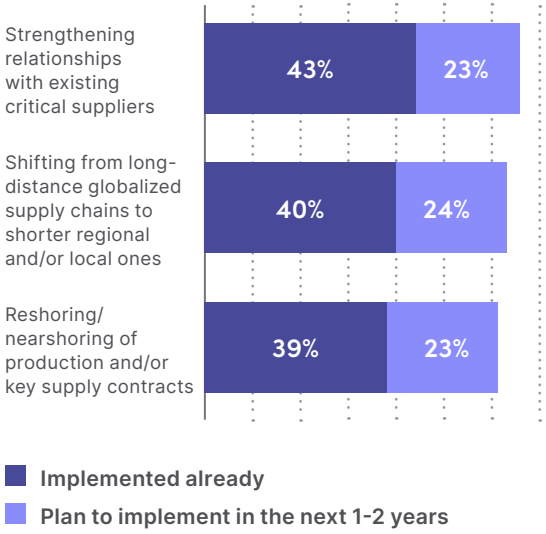
85%

of participants are "extremely" or "somewhat" concerned about geopolitical tensions

Top concerns from a geopolitical perspective:

1. Difficulty in getting supplies of essential raw materials, components, products, and/or energy
2. Damage to cost efficiency from resilience-building measures
3. Increasing government focus on protectionism, national security, industrial policy and/or self-sufficiency

Top three resilience strategies organizations have implemented or plan to implement, in response to geopolitical risks and events



Better Relationships, Local Supply Key to Resilience

Organizations have responded to geopolitical events and risks, as they did the during the pandemic, by restructuring their global supply chains. A clear majority have either already moved to more regional or national suppliers and operations, or plan to do so in the next couple of years, with healthcare firms especially active. The same is true for reshoring or nearshoring key supply contracts (led by A&D and energy companies) and diversifying global footprints – in particular, moving some suppliers and/or production away from China to other countries. Organizations are also diversifying their range of supply options through a greater use of dual- and multi-sourcing.

The additional costs of resilience partly explains why strengthening relationships with existing critical suppliers is the most common resilience strategy, since it is perceived as requiring less financial investment. At the same time, suppliers have a critical part to play in managing geopolitical and other risks and ensuring greater operational resilience. There is only so much one organization can do alone: collaboration with ecosystem partners is essential.

> "We are looking at nearshoring and consolidating which parts of the world we are sourcing product, but certain raw materials (titanium, special metals, composites) can only be obtained in a small number of countries."
>
> – **Procurement Leader,** Aerospace & Defense, U.S.

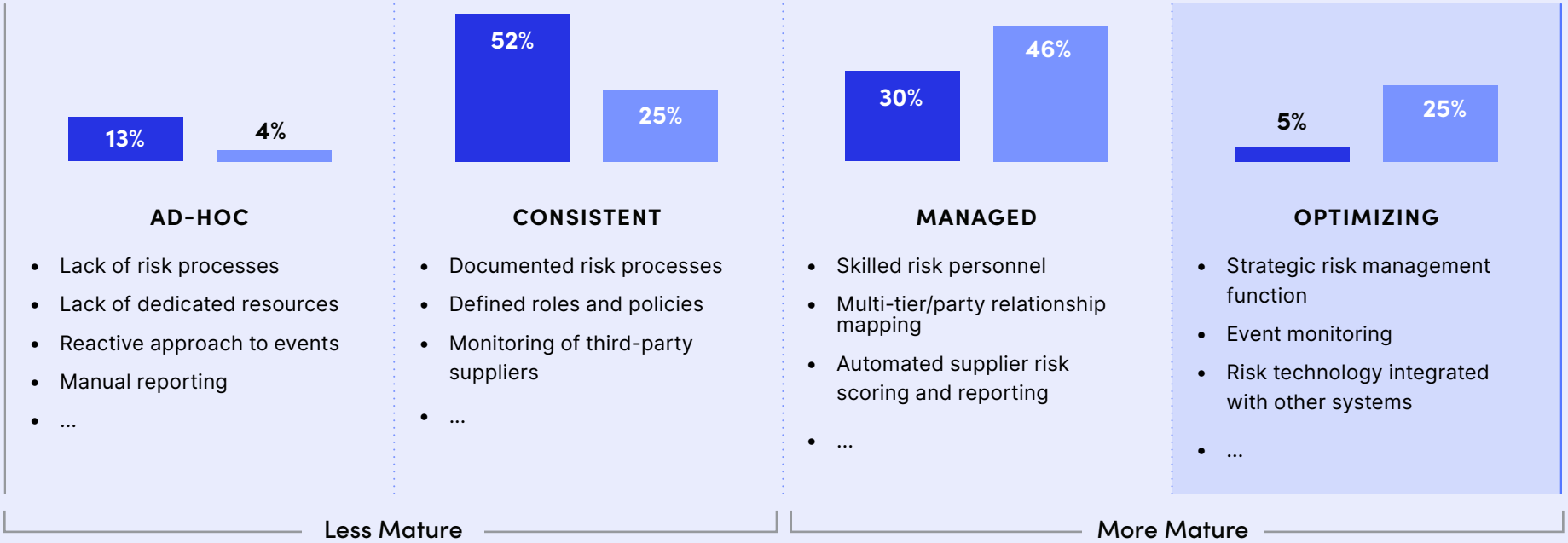
SECTION 02

The State of Supply Chain and Third-Party Risk Management

Maturity Set to Increase in Next Three Years

Despite being impacted by major disruptions, such as COVID-19 and the Ukraine war, many organizations still lack the knowledge, resources, processes and tools needed to manage supply chain or third-party risks and respond effectively to large-scale incidents. Almost all (95%) of procurement executives do not think they have reached the final stage of SCRM/TPRM maturity. Additionally, almost two-thirds (65%) self-identify their organizations at a lower stage of maturity today – specifically, as “ad-hoc” or “consistent” on the Interos SCRM/TPRM maturity scale – compared with just over one-third (35%) who rate themselves as more mature, defined as “managed” or “optimizing”.

Interos SCRM/TPRM Maturity Scale



(Above)
Q: Overall, how would you describe your organization's maturity in SCRM or TPRM terms against the following scale?

Today

In the next 3 years

However, asked where they expect to be in three years and that balance more than reverses, with 71% expecting to be at the mature end of the spectrum. At this level, organizations manage risk proactively and strategically, with capabilities that include:

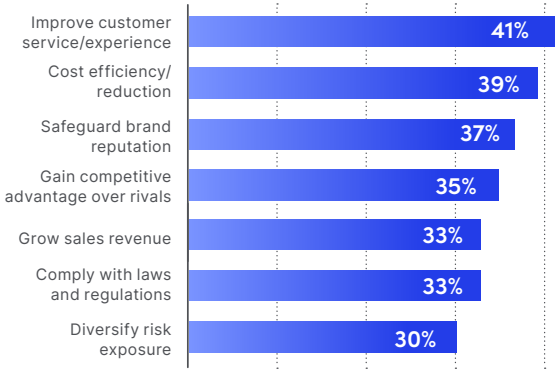
- A dedicated SCRM/TPRM function
- Skilled risk management personnel
- Agreed processes and effective internal collaboration around these
- Multi-tier visibility of the extended supply base
- Automated supplier risk assessments and executive reporting
- Continuous monitoring of potentially disruptive events

Diving deeper into the data reveals that organizations with higher annual revenue were three to six times more likely to consider themselves optimizing than smaller organizations.

"The adoption of TPRM has been slow. Corporate-wide digital transformation initiatives are now making things easier, but it is a long road."

– Procurement Leader,
Aerospace & Defense, U.S.

Q: What is the main business driver(s) for developing and implementing SCRM/TPRM in your organization?



Maturity Levels Today Vary Widely Between Sectors

The overall findings mask some stark differences between industry sectors. Almost half of A&D firms place themselves in one of the two mature categories today, compared with just over one-fifth of government organizations. This is notable, since central government is the primary customer for defense equipment manufactured by A&D suppliers. At a broad sector level, it suggests a significant imbalance in the ability of each party to manage supply chain risks effectively.

That said, government agencies are more optimistic than either healthcare or energy companies in terms of where they plan to get to in the next three years. And they expect to close the gap with A&D. Almost 7/10 (69%) of government agencies reckon they will progress their SCRM and TPRM capabilities to the managed or optimizing level during this period, compared with 83% of A&D firms.

Top Drivers: Customer Service, Cost Efficiency

Regardless of the differences, the ambition to improve risk management practices exists across all sectors surveyed. What is driving this need for change? The data shows that improving customer service and the customer experience is the most common business driver for better SCRM/TPRM. This is unsurprising given that supply chain disruptions can lead to customer orders being delayed, promises broken and trust damaged – civil airliners and new passenger cars being just two current examples. But the need to manage costs efficiently – and to reduce that $82 million annual average bill – is a close second for CPOs and their teams.

It is notable that more mature organizations are driven less by cost-efficiency/reduction and more by brand reputation, competitive advantage and growing sales revenue.

Better Risk Management Has Financial Benefits

Asked to estimate the financial value of better risk management, almost three-quarters of participants picked an annual figure of between $10 million and $50 million, with the mean average being $37 million. This includes both cost savings and higher sales (a risk improvement driver for one-third of our sample) and equates to 45% of the average cost of supply chain disruptions in 2022. As with maturity, A&D firms are the most optimistic about the potential financial benefits of SCRM/TPRM ($47 million on average) and government organizations the least ($26 million).

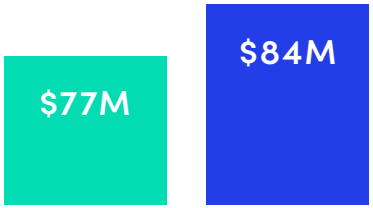
It is also worth noting that while those leaders identifying as more mature today estimate the same average potential benefits figure of $37 million as their less mature peers, they also report a lower average cost of disruption ($77 million versus $84 million). So higher levels of risk management maturity are associated with lower disruption costs and, any additional SCRM/TPRM program running costs notwithstanding, a better overall financial equation.

Participants who reported a higher perceived financial benefit to reacting faster, experience more disruptions.

> "The reason we have a global supply chain is to give us a competitive advantage. But a global supply chain increases the potential risk to quality, reliability and our reputation. SCRM reduces our exposure to these factors."
>
> – **Procurement Leader,** Aerospace & Defense, U.S.

$37M

Estimated annual cost savings and/or revenue improvement from being better prepared and able to react faster to supply chain disruptions



Annual **cost of supply chain disruptions** for more mature organizations versus less mature

- Mature
- Less mature

> "Our supply chain has to be seen as providing us with a competitive advantage. We have to provide end-to-end planning, visibility and collaboration."
>
> **– Procurement Leader,**
> Aerospace & Defense, U.S.

Top three challenges organizations face in pursuing ESG goals with both direct and indirect suppliers

1	Lack of reliable data to inform goal-setting and progress tracking	42%
2	Lack of visibility into subtiers of extended supply chains	42%
3	Procurement organization has more pressing priorities	39%

ESG is Core to Safeguarding Brand Reputation

More than one-third (37%) of our survey sample identified safeguarding brand reputation as a business driver for better risk management. Environmental, social and governance (ESG) initiatives are one of the main methods organizations use to protect and enhance their brands among customers, employees, investors and other stakeholders these days. Just over half (51%) of procurement leaders acknowledge that their efforts, while important, have taken a backseat for the time being owing to cost and supply availability issues taking precedence in their departments.

At the same time, 35% say they are stepping up their ESG supply chain activities and investments. This trend is most pronounced among financial services and healthcare firms, and among those with more mature SCRM/TPRM capabilities (45% stepping things up compared with just 29% of less mature organizations). Interestingly, despite the growing importance of ESG issues on the political agenda, just 18% of government agencies said they were increasing their investments here.

Specific areas where progress with suppliers is reported to have made the greatest strides during the past three years include:

- Renewable energy
- Recycling and reuse of materials
- Working conditions

Top ESG Challenges: Usable Data, Sub-Tier Visibility

Despite the importance of ESG objectives to organizations and supply chain/third-party risk managers, significant challenges remain when it comes to pursuing improvement initiatives with suppliers. Aside from competing priorities and budget constraints, the two most often identified by CPOs are a lack of reliable data and sub-tier visibility. Both are critical in the ESG domain, where violations of environmental and social standards can, and often do, occur further upstream in the supply chain among suppliers with whom an organization is only indirectly connected.

Q: Thinking about the regulations around supply chain/ third-party risk and operational resilience, do you agree with the following statements?	Percentage that Agree
These laws impose **a heavy burden** on our organization in terms of additional cost, time, data, and resources required to comply	79%
We cannot hope to comply effectively with these laws without supporting **data, analytics and risk management software**	74%
New regulatory requirements help us to improve collaboration and information sharing with our **direct (tier-1 or third-party) suppliers**	74%
New regulatory requirements force us to improve our awareness of critical **indirect (e.g., tier-2/3 or fourth/fifth party) suppliers**	74%

Regulations Promote Better Risk Management

Complying with a growing body of laws and regulations is now a fundamental part of the fabric of ESG risk management, as it with cybersecurity and broader operational resilience programs. So it should be no surprise that one-third of survey respondents listed compliance as a top 3 business driver for SCRM/TPRM.

While 79% agree that legislation imposes “a heavy burden” on their organizations from a cost, time, data and resources standpoint, the findings show it also acts as a development spur for risk management capabilities.

The same percentage say that new laws compel them to invest in risk processes, people and technology – something that almost three-quarters agree they must have to ensure compliance. Seven out of 10 go further than simply compliance, however, welcoming stricter laws on the grounds that they present an opportunity to gain competitive advantage against rivals.

Regulations Promote Collaboration and Awareness

Similar numbers of procurement heads believe that regulations force them to improve the way they collaborate with other functions, such as IT security, legal, supply chain and sustainability, as well as with external suppliers and partners. The need for better collaboration and information sharing, both inside and outside the organization, was identified as a key improvement priority in the **2022 Resilience report**.

Cyber, ESG and other laws also force organizations to improve their visibility of critical direct and indirect suppliers, according to 74% of survey participants. This is an essential foundation for maturing SCRM/TPRM capabilities and driving greater operational resilience, as we explain in the next section.

SECTION 03

Developing Operational Resilience

Supply chain and third-party risk management is an important component of operational resilience. To achieve this, risk leaders need to do three things:

1. **Map** their supply chains and understand key dependencies and relationships at multiple tiers/parties

2. **Model** their risks and pinpoint key areas of potential disruption that need to be mitigated in advance

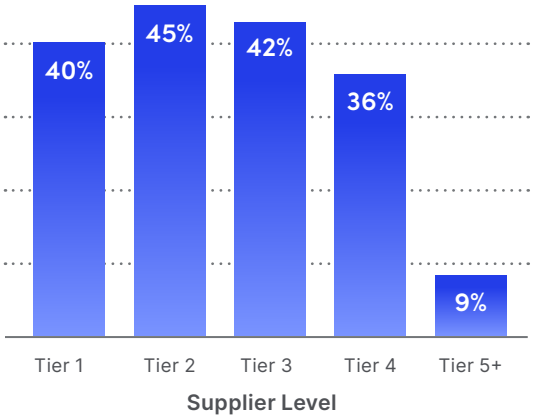
3. **Monitor** events across their global networks in real time or near real time, so they can react quickly when required

Mapping, modelling and monitoring are important parts of an ecosystem-based approach to supply chain and third-party risk management: one that is designed to identify issues and potential sources of disruption earlier and respond sooner and more effectively when an event occurs.

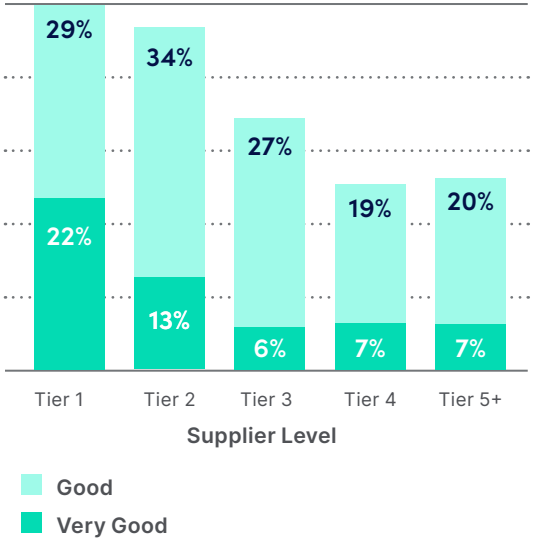
How Interos Defines Operational Resilience

Operational resilience is the ability to continue providing products or services in the face of adverse market or supply chain events. An operationally resilient organization manages risk in a strategic and proactive way to prevent, respond to and recover quickly from disruptions that could impact its customers, brand reputation or financial performance, and to seize new business opportunities.

Origin of disruptions



Level of Visibility



1. Multi-Tier Relationships Need to Be Mapped

Mapping at multiple tiers, or parties, is the foundation of operational resilience. If enterprises don't know who they are doing business with – both directly and indirectly – and where those companies are located, it is almost impossible to proactively manage risk and make smart choices about where to invest in contingency options.

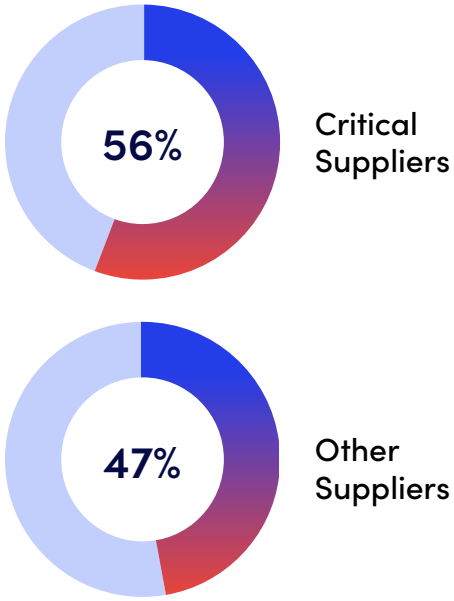
Disruptive supply chain events – whether a supplier bankruptcy, a factory fire, a cyber attack or another incident – often originate among sub-tier or nth-party suppliers. Our survey data shows that in the past 12 months tier-2 or fourth-party suppliers were the most common source, followed by those at tier-3/fifth parties. However, visibility at these indirect levels of the extended supply chain were less than complete. At tier 2, less than half (47%) of executives expressed confidence that they had "good" or "very good" visibility (where good was defined as having knowledge of more than three-quarters of firms, their locations and the products or services they provide). At tiers 3, 4 and 5+, one-third or less believed they had this degree of information.

Organizations with more mature supply chain/third-party risk capabilities claim slightly higher levels of visibility, but even here there is plenty of room for improvement.

For example, A&D firms were 16-19% more likely to say they had good/very good visibility across tiers 1, 2 and 3 than the average for all organizations. But they fell back in line when it came to tiers 4 and 5+. So there is room for improvement even among those with more mature capabilities.

> "Use technology tools to enhance visibility and transparency in the supply chain and third-party relationships."
>
> **– Procurement Leader,** Energy & Utilities, U.K. & Ireland

Mean percentage of an organization's suppliers subjected to a risk assessment during the sourcing and/or supplier management process



2. Risk Assessments Must Cover More Suppliers

Understanding relationships and dependencies at different levels of the supply chain is an essential step in determining where weaknesses and vulnerabilities exist that may need to be addressed through mitigation strategies. But an organization also needs to know how risky individual suppliers are and in which specific dimensions. The risk assessment component of modeling addresses this, providing information that procurement and risk managers use for decision making and prioritization.

Survey participants were asked to distinguish between "critical" suppliers – those that are especially important to business units, provide essential products and services, have good strategic fit with their customer, and so on – and "other" suppliers. On average, 56% of critical suppliers and 47% of other suppliers are subjected to a risk assessment during the sourcing and/or supplier management process. Coverage is somewhat better in the A&D sector and among more mature and larger organizations, but even here the figures are relatively low compared with where they should be for security, compliance and operational resilience purposes.

> "A TPRM system allows you to rank your suppliers in importance and perceived risk. The suppliers who are critical to your company must be accurately assessed."
>
> **– Procurement Leader,** Aerospace & Defense, U.K. & Ireland

3. Risk Monitoring Needs to Be Continuous

Conducting due diligence and checking certifications during the supplier selection process, and then auditing key suppliers to validate policies and practices (for example, around ESG) during the contractual relationship are necessary parts of effective supply chain and third-party risk management. But in a dynamic, fast-changing risk landscape, these periodic interventions are not sufficient to get ahead of and respond quickly to disruptive events. For this, organizations need continuous monitoring across their extended supply chains.

Just 7% of procurement leaders say they monitor their most critical suppliers on a daily basis, with 17% saying they do it weekly (more mature organizations are slightly higher on both frequencies). The majority (59%) conduct risk monitoring on a quarterly or biannual basis. For other suppliers, the frequencies are lower still, with almost one-quarter saying they only do this once a year. On average, critical suppliers are monitored every 20 weeks and other suppliers every 26 weeks. This leaves organizations vulnerable to unexpected and unpredictable risk events.

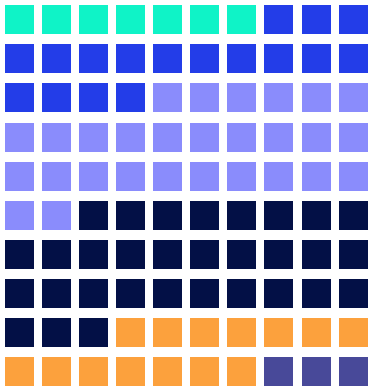
When looking at the data across industries, government organizations reported assessing critical suppliers least frequently – every 25 weeks – while financial services firms assessed critical suppliers every 17 weeks on average.

Notably, organizations that reported having positive economic expectations for 2023 assessed critical suppliers much more frequently (every 18 weeks) compared to those with negative expectations for the year (every 29 weeks).

> "It is essential that organizations can effectively manage supply chain risk to increase certainty and avoid dangerous surprises."

– Procurement Leader,
Central Government, U.K. & Ireland

Q: How frequently does your organization monitor supplier risks and potential disruptions during the post-contract commercial relationship for critical suppliers?



- Daily - **7%**
- Weekly - **17%**
- Quarterly - **28%**
- Every six months - **31%**
- Annually - **14%**
- Ad Hoc - **3%**
- Never - **0%**

Percentage of respondents who would currently be aware of a supplier disruption within 48 hours across all tiers of their supply chain.

Supplier...	
...suffers a cyber attack	1%
...commits an ESG violation	3%
...becomes financially insolvent	3%
...disrupted by a geopolitical issue	2%
...experiences an operational disruption	3%
...disrupted by extreme weather/natural catastrophe	4%
...becomes the subject of a restriction/ sanction	3%

4. Risk Event Awareness Requires Improvement

Early awareness and notification of supplier risk events at different supply chain tiers is vital for customer organizations to respond appropriately (including through pre-defined mitigation plans) and limit any negative impact. The first few days after an incident happens can be an important window for situation assessment and taking any necessary actions. These might include securing spare manufacturing capacity, switching orders to a different supplier, acquiring available supply on the open market, and re-routing logistics.

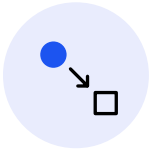
Less than 5% of procurement leaders say they have enough visibility to be aware of various risk events within 48 hours of occurrence across every tier of their supply chain. A significant minority – and close to half in the case cyber attacks, financial insolvencies or new restrictions being applied – say they need to make "significant" or "major" improvements to ensure they know about events within 48 hours. "Significant improvement" equates to no visibility at any tier of their supply chains, while "major improvement" was defined as only having confidence with tier-1 or third-party suppliers.

A further one-third of our sample say they need to make "moderate" improvements – that is to say, they believe they would be aware of events at, say, tiers 1 and 2 within 48 hours, but not tiers 3, 4 or 5.

Again, maturity plays a role here. More mature SCRM/TPRM organizations were 23%–34% more likely to say that they would have 48-hour notification of cyber, operational, financial or geopolitical events at the lower tiers of their supply chains than those that are less mature today.

The areas where executives want to significantly or moderately increase investments this year

52%
People



56%
Processes

53%
Technology

5. Invest in Risk People, Processes and Technology

Improving SCRM and TPRM capabilities demands a mixture of people, process and technology. Despite an uncertain and, in some sectors, challenging economic environment, procurement leaders are generally optimistic about the remainder of 2023, with upwards of 80% positive about their organizations' financial outlook. (The exception is federal and central government, where 49% are negative). This optimism translates into expectations about the resources they are likely to have to manage risk. The majority expects to grow their investments in people, process and technology this year, while between 22% and 30% say spending will be flat in each of the three areas.

More mature organizations are more likely to say they are significantly increasing their investments in technology this year, as they are with both people and process.

> "Successful risk management requires a change in approach and attitude. It needs to embrace innovation in procurement and enable new technology."
>
> – **Procurement Leader,** Federal Government, U.S.

Top three benefits of SCRM and TPRM technology solutions

Identifying risky suppliers across multiple factors

Data/analytical support for risk mitigation

Multi-tier supplier relationship visibility

Top Tech Benefits: Risk Spotting, Decision Support

The two greatest operational benefits of SCRM and TPRM technology solutions in the eye of CPOs are: the ability to identify high-risk suppliers, and data/analytical support for decision making (including risk mitigation actions). But just six points separate these benefits from others that respondents were asked to select from for their top 3 – namely, identifying risky suppliers across multiple factors, data/analytical support for risk mitigation, and multi-tier supplier relationship visibility.

From an industry vantage point, aerospace & defense and energy organizations were more likely to consider the ability to identify high-risk suppliers across multiple factors the key benefit of technology than other industries. Additionally, organizations with more mature SCRM/TPRM programs were more likely than less-mature organizations to care about better executive reporting and multi-tier relationship visibility.

No executive out of the 750 surveyed said they saw no benefits from using technology for risk management.

> "We use advanced data analytics, allowing us to take fast action and make decisions based on events as they happen."
>
> – **Procurement Leader,** Aerospace & Defense, U.S.

SECTION 04

Recommendations

- **Invest in continuous, multi-tier supply chain risk visibility.** Only 7% of companies continuously monitor their suppliers, and most lack good visibility of all of the tiers within their supply chains. Without this level of insight, companies are relying on point-in-time snapshots that leave them vulnerable to disruption, and lagging behind competitors and peers who have begun to seize on the advantage comprehensive visibility provides.
- **Apply a maturity model and track progress against it.** More mature organizations have lower costs associated with disruption and better visibility of their supply chain – yet 95% of companies think they need to improve their risk management capabilities. To start realizing these benefits, organizations need to begin investing in documented processes, strategic risk functions, skilled personnel, and risk technologies that are integrated with their key systems.
- **Develop proactive resilience and reactive response capabilities.** Resilience demands upfront strategic analysis and planning, combined with the agility to respond quickly when a disruptive risk event strikes. Currently, far too many firms don't know about a supplier disruption in the first 48 hours - and time is money. Investments to achieve this readiness need to be weighed carefully and will vary between organizations according to the nature of their business, their size, profitability and appetite for risk.

> “With the right analysis, planning and technology, operational resilience can be efficiently secured.”
>
> **– Procurement Leader,**
> Energy & Utilities, U.S.

- **Forge internal collaboration between risk owners and functions.** Overall responsibility for managing supplier risk may rest most naturally with the procurement function (and does for 35% of our survey sample), but ESG, cyber, financial and other risks are often jointly owned. Alignment and collaboration between procurement and other corporate functions – IT security, finance, legal, supply chain, sustainability, enterprise risk management, operational resilience, etc. – therefore needs to be tight and effective.
- **Cultivate critical supplier relationships across your ecosystem.** Collaboration with external partners is vital in managing a global, multi-tier risk network – strengthening relationships with existing critical suppliers was the most-selected resilience strategy in our survey. This means information sharing, and in some cases, shared investments to mitigate the most critical risks. All of this is more difficult, if not impossible, to achieve without a corresponding level of open communication and trust between buyer and supplier.
- **Harness technology for efficiency and actionable intelligence.** In larger organizations, modern-day SCRM and TRPM are too complex to be run using spreadsheets. Advanced software and data analytical capabilities are essential for identifying, assessing, mitigating and monitoring supply chain risks on a continuous basis. It is not surprising that a majority of respondents plan to increase their investment in technology this year. Effective supplier risk specialists spend the bulk of their time preparing their organizations for and responding to impactful events, not gathering data.

interos

About Interos

Interos is the operational resilience company. We are reinventing how companies manage their supply chains and business relationships through a breakthrough SaaS platform that uses artificial intelligence to model and transform the ecosystems of complex businesses into a living global map, down to any single supplier, anywhere. Reducing months of backward-looking manual spreadsheet inputs to instant visualizations and continuous monitoring, the Interos Operational Resilience Cloud helps the world's companies reduce risk, avoid disruptions, and achieve superior enterprise adaptability. Businesses can also uncover game-changing opportunities to radically change the way they see, learn and profit from their relationships.

Contact us today to schedule a demonstration

Request Contact

For more information:
www.interos.ai or 1 (703) 745-5578

080923