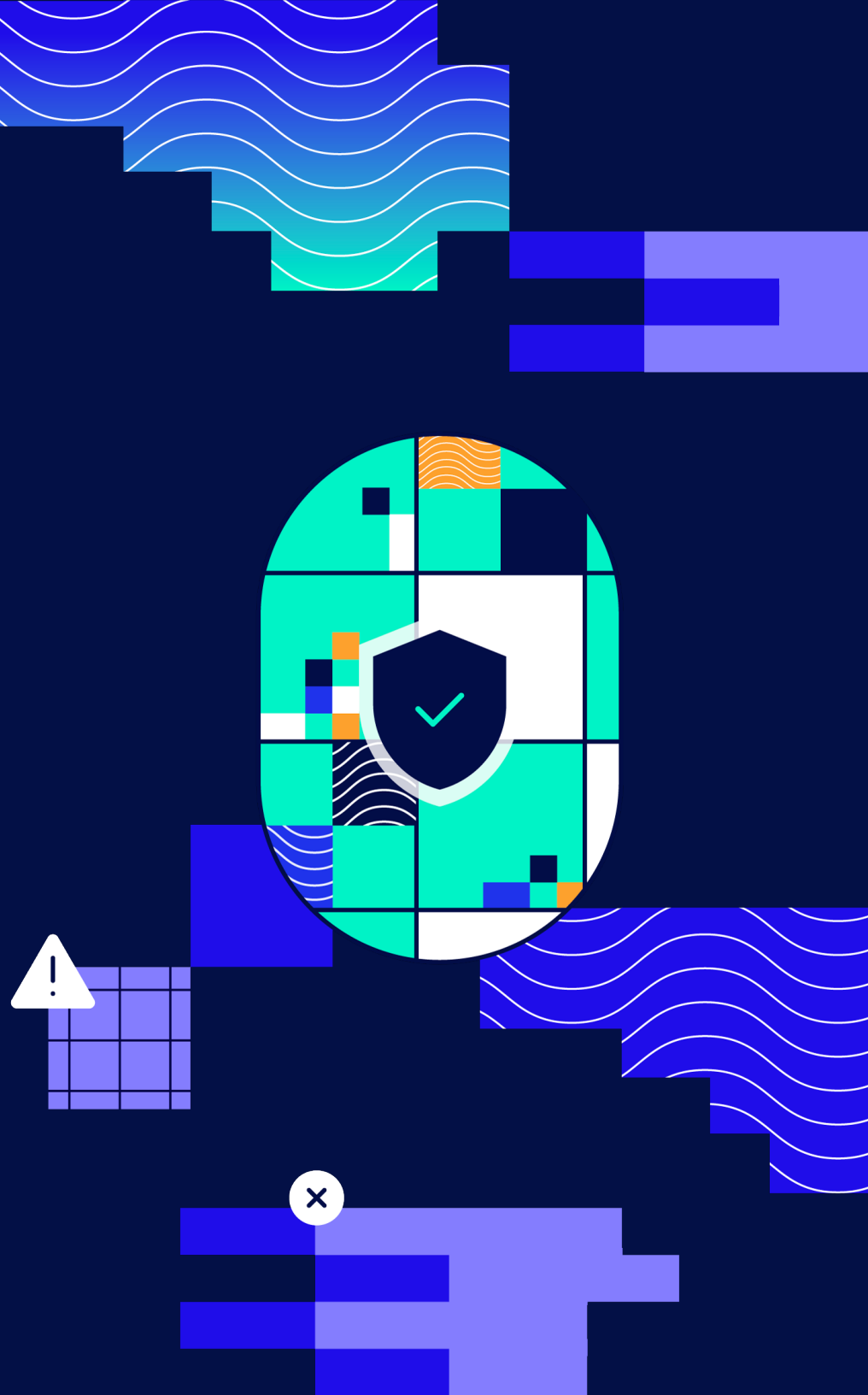
interos

THE THIRD ANNUAL INTEROS SUPPLY CHAIN SURVEY

Invisible Threats: Resilience 2023

Government Imperatives



interos.ai

Table of Contents

Foreword

“Supply chain resilience is more than just a response to disruption; it’s the proactive pursuit of change through a strategy known as Resilience by Design™. The Interos Resilience Survey is an annual benchmark created to assist organizations in their journey toward this goal. Developed by independent researchers, it’s the only industry report to quantify the impact of multifactor risk on global supply chains.

This year’s results for government organizations highlight how even public institutions are caught in the throes of turbulent economic forces. Agencies continue to wrestle with cyber-attacks, rising geopolitical tensions, and increasing natural disasters. Leaders agree there is an urgent need to move from lagging to leading risk indicators to foster a more rigorous and anticipatory approach to resilience – and many are turning to technology for the solution.

In a world where adaptability is key to performance, AI technologies and a designed approach to resilience enable leaders to act five days sooner, think five moves ahead, and see five layers deeper to prevent disruption and secure the mission.

Combined with the right people and process – organizations are increasingly committed to evolving supply chain risk management (SCRM) and third-party risk management (TPRM) from checkbox compliance into an engine for long-term value creation building brand, reputation, and profitability.

Collaboration is paramount too, both internally and externally. While procurement naturally manages supplier risk, other functions like operations and enterprise risk management also 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 automate processes.

Resilience by Design™ is only achievable through a willingness to leave behind strategies that no longer work. By prioritizing visibility, proactive risk elimination, and sustainability, we can ensure that our most vital public institutions, and the industrial base supporting them, can maintain mission-readiness in a turbulent world.”

JENNIFER BISCEGLIE,
Interos Founder & CEO

Overview

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

This year, we surveyed 150 senior supply chain, procurement, and third-party risk decision makers across central/federal government organizations in the U.S., U.K., and Canada to understand how changing industry dynamics are impacting TPRM/SCRM – bringing new insights, trends, and best practices for supply chain risk and procurement professionals.

While the overall cost of disruption has waned post-pandemic, the drive to increase cost-efficiency while complying with increasingly complex regulations and maintaining mission-readiness is driving government organizations to advance TPRM/SCRM maturity.

It's important to note this research was conducted independently, with no mention of Interos.

In their responses government leaders made clear that a rise in natural disasters and geopolitical turmoil have increased uncertainty over their supply chains – and that the drive to lead the way on resilience and reliability requires continued investment and unwavering vigilance.

Key Findings

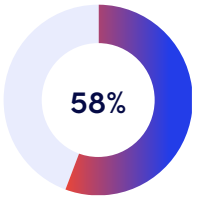
4

The average government organization experiences **four supply chain shocks requiring** "significant mitigating action" annually

↑$26M

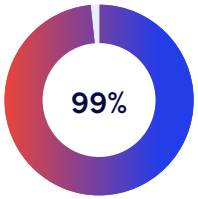
Government organizations believe they **can recover $26M annually** by preparing better for and reacting faster to disruption

RISK ASSESSMENT



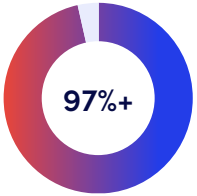
On average, government organizations only assess 58% of their critical suppliers for risk

RISK MANAGEMENT MATURITY



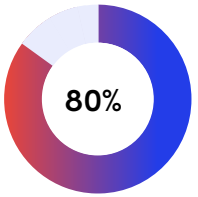
99% of government organizations do not consider themselves to have reached the highest level of SCRM/TPRM maturity

EVENT AWARENESS



97%+ of government organizations say they would not be aware of a supplier disruption in all the tiers of their supply chain within **48 hours of occurrence** (varies by disruption type)

DATA, ANALYTICS AND SOFTWARE



80% of government procurement leaders agree that they cannot comply with emerging regulations without supporting data, analytics, and risk management software

Out of the

150

Senior procurement leaders we surveyed...

81 are from the **United States**

38 are from the **UK and Ireland**

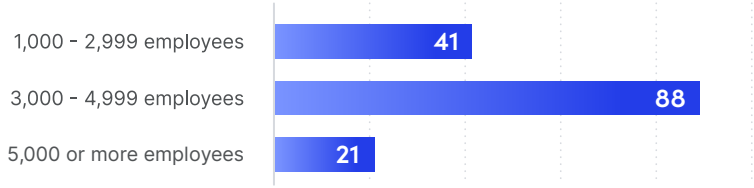
31 are from **Canada**

132 are within senior management

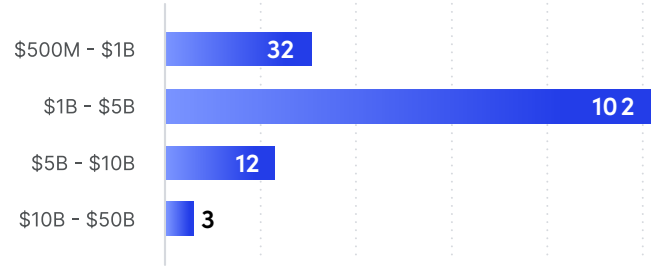
18 are C-level or board members

Demographics

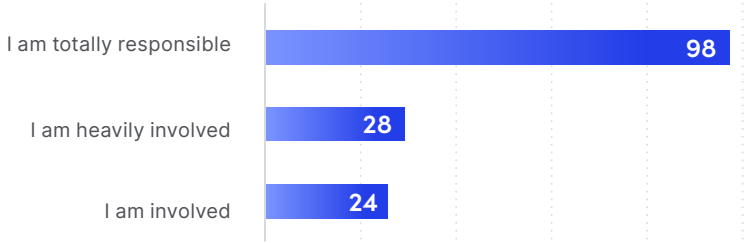
Q: How many employees does your organization have globally?



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

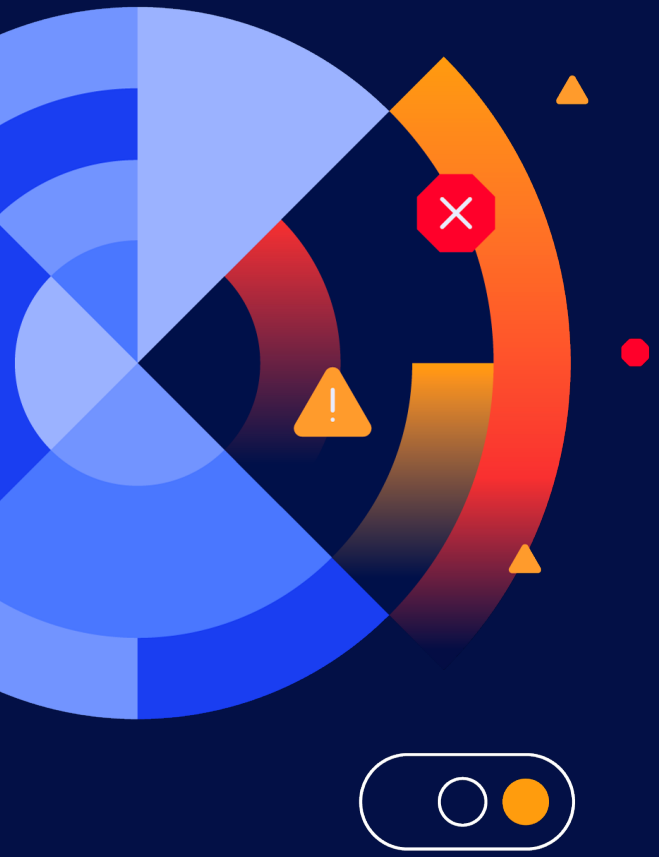


Q: What is your level of involvement when it comes to managing the global supply chain in your organization?



SECTION 01

Navigating the Maze of Supply Chain Disruption



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

The havoc wrought by COVID-19 may have subsided during the past year, but plenty of other disruptive events continue to impact the supply chains of government organizations and the defense industrial base (DIB) in 2023. They include:

- Russia's ongoing war in Ukraine
- Rising geopolitical tensions between the U.S. and its allies and China, including the threat China poses to semiconductor powerhouse Taiwan
- Sanctions, export controls and other restrictions on Russian and Chinese entities, including those that could curtail access to advanced technologies such as new semiconductors.
- Soaring costs in energy, food and a wide range of commodities and services
- A relentless 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

Decoding the Costs of Frequent Disruptions: A $54M Gap

Supply chain disruptions are frequent, costly, and mission-threatening. In total, 150 government organizations participated in the study. On average each lost a total of $54M responding to four major supply chain disruptions within the past 12 months - to say nothing of the impact on mission-readiness. These were events requiring “significant mitigating action.” Mitigation included activating alternative suppliers, shifting production lines, utilizing buffer inventory, or revising delivery schedules.

Survey data revealed that aerospace & defense firms suffered significantly lower losses due to supply chain disruption than all other sectors excepting government organizations (between $27M - $38M less).

> “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,** U.S.

4

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

$54M

Annual financial impact as a result of these supply chain disruptions

$13M

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

$96M

Average annual cost of disruption for government organizations with $10B - $50B in annual budget/revenue

$28M

Average annual cost of disruption for government organizations with $500M - $1B in annual budget/revenue

Costs by Vertical (in USD millions)

Survey data revealed that government organizations suffered significantly lower losses due to supply chain disruption than all other sectors surveyed (between $11M - $48M less). The next-lowest industry was aerospace & defense, while financial services respondents reported the greatest losses.

This disparity may reflect the fact that, when government organizations are hit by supply chain disruption, the cost in dollars does not tell the full story. These organizations provide essential public services which supply chain disruptions often significantly impact – impairing mission delivery but not always affecting their finances. Government agencies are also less demand-sensitive than commercial organizations, with demand driven more by long-term contracts and federal policy, than immediate consumer need.

Conversely, financial services, energy, and healthcare organizations often rely heavily on sprawling digital networks for data processing and transaction support – making them more vulnerable to global disruption.

Smaller government organizations (those with between $500M - $1B in annual budget/revenue) lost an average of ~4% ($28M) of their budget to supply chain disruption. On the other end of the scale, larger organizations (those with between $10B - $50B in annual budget/revenue) lost ~3% ($96M) on average. This indicates that the cost of disruption for government organizations scales closely with the size of that organization's budget.

This stands in contrast to other industries surveyed, where smaller organizations lost a greater percentage of their revenue to disruption – potentially indicating that government organizations/agencies have achieved greater standardization in their risk management practices. However, as mentioned above, when it comes to federal organizations – direct costs only tell part of the story. For many organizations, even small, unexpected costs can impact mission-delivery.

> "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,** U.S.

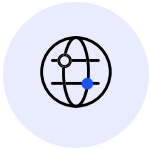
Q: What annual cost increases and/or revenue losses does your organization experience annually?

FINANCIAL

$44M

CATASTROPHIC

$47M



GEOPOLITICAL

$45M

CYBER

$43M

ESG

$45M

RESTRICTIONS

$51M

Shocks to the System: Six Major Categories of Risk

When we look at losses connected to different types of supply chain disruption – new patterns emerge. Procurement leaders at government organizations reported annual cost increases and/or financial losses ranging from $43M to $51M in each of six distinct risk categories:

- **Financial**, including supplier health, insolvency, liquidity
- **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 physical and digital infrastructure
- **ESG,** including environmental factors such as carbon emissions and pollution, and socio-economic 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 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,** 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**, U.S.

45%

of government organizations put supply shortages in their top 5 risks

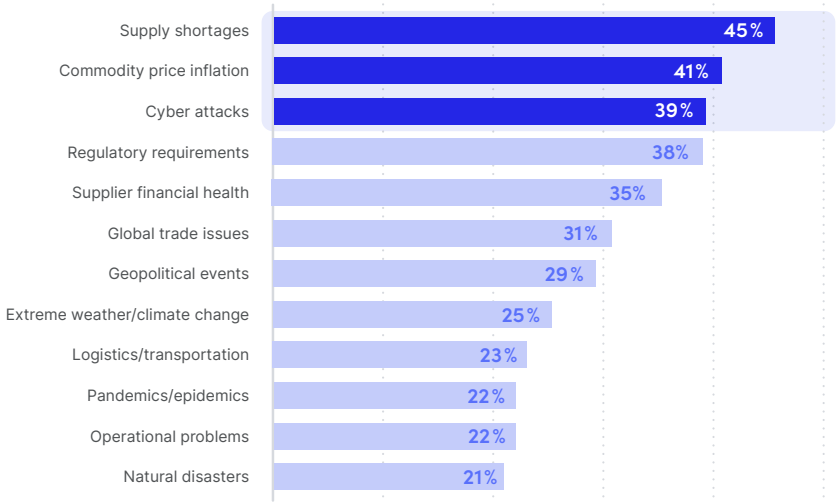
Top Crisis Triggers: Supply Shortages, Inflation, Cyber-Attacks

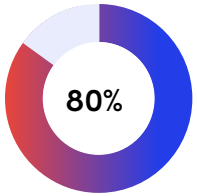
Supply shortages, inflation, and cyber-attacks top the list of concerns for government procurement leaders by a slim margin – indicating the threats these specific risks pose to mission-readiness, as well as the frequency with which they impact government organizations and/or the DIB. While government organizations are near-equally concerned about the array of threats that face, they are less concerned about certain issues such as pandemics and natural disasters, reflecting the reduced impact of COVID-19, compared to 2-3 years ago.

Government leaders were between 10% - 18% more likely to be concerned about the impact of supply shortages, inflation, and cyber-attacks on their supply chains than those in financial services, healthcare, and energy.

These elevated levels of concern reflect the criticality and sensitivity of the work of government organizations, the frequency with which they are targeted, and their reliance on many small-medium sized businesses who may be more vulnerable. For example, a successful cyberattack on a key component supplier could have dire implications for national security, classified data, or advanced military technologies.

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)





80% of government respondents agreed they "cannot hope to comply with these laws without supporting data, analytics and risk management software"

	Regulation	Impact*
	OSFI B-10 TPRM Guideline	69%
	Uyghur Forced Labor Prevention Act (UFLPA)	72%
	National Defense Authorization Act (NDAA) Sections 889/5949	72%
	Interagency Guidance on Third-Party Relationships – US	70%
	German Supply Chain Due Diligence Act	61%
	Corporate Sustainability Due Diligence Directive (CSDDD)	66%
	Digital Operational Resilience Act (DORA)	65%
	Critical Raw Materials Act – EU (proposed)	64%
	PRA/FCA Operational Resilience Regulations	67%

* Significant or moderate impact

Expanding Regulation: Legislation Will Have a Material Impact

Regulatory requirements are another key 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 cybersecurity and operational resilience. A slew of others are also in the pipeline.

When asked about a variety of supply chain regulations, government organizations were generally less concerned over the issue than most of the industries we surveyed – excepting aerospace & defense. Specifically, government organizations were between 10% - 19% less likely than the cross-industry average to say that the regulations we asked about would have a significant/moderate impact on them.

Government organizations had the lowest level of concern out of all the industries we surveyed over two regulations that, overall polled the highest: Sections 889/5949 of the National Defense Authorization Act (NDAA), and the Uyghur Forced Labor Prevention Act (UFLPA). Government leaders may have comparatively diminished concerns over adhering to these regulations because they are often the entities responsible for implementing, overseeing, and enforcing such regulations, giving them a more in-depth understanding and preparedness regarding compliance requirements.

80% of government respondents agreed they "cannot hope to comply effectively with these laws without supporting data, analytics and risk management software." Some controls are also perceived as beneficial over the long term. 85% of government respondents consider legislation helpful in forcing organizations to improve supply chain and third-party risk management capabilities, as do similar percentages of other the other verticals surveyed.

Shortages, Costs, Protectionism Are Top Geopolitical 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 escalation 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 for all industries.

When asked specifically about the potential impact of geopolitical tensions on their suppliers and supply chains over the next three years, 88% of government participants say they are "extremely" or "somewhat" concerned.

Difficulties in getting essential raw materials/components are uppermost in government CPO's minds. They are also concerned about the potential cost increases due to geopolitical disruption. Government leaders also have concerns over how government industrial and national security policies are reshaping global trade in a more protectionist direction. These concerns were broadly shared among other verticals.

As we'll see later in the report, increasing supply chain visibility may be the missing piece leaders need.

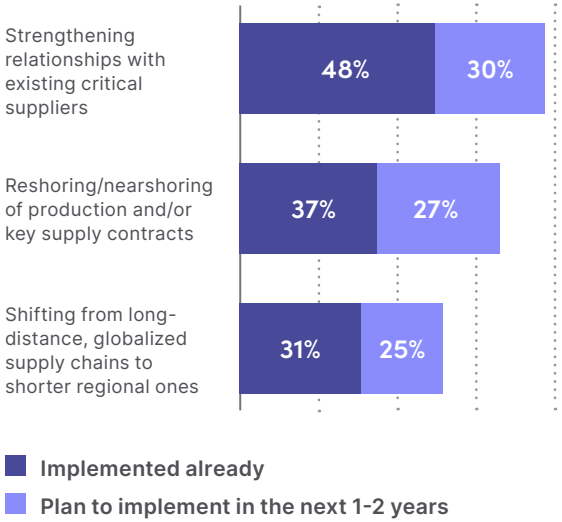
88%

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

Top concerns from a geopolitical perspective:

1. Difficulty in getting supplies of essential raw materials
2. Cost increases as a result of geopolitical events
3. Increasing government focus on protectionism, national security, industrial policy and/ or self-sufficiency

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



Better Relationships and Reshoring/Nearshoring Key to Resilience

Government organizations have restructured their global supply chains and supplier networks in response to geopolitical risk events. A majority of government organizations (as well as organizations across industry) have met this challenge by reshoring or nearshoring key supply contracts and shifting supply chains from long-distance/globalized supply chains to local ones. This includes moving some suppliers and/or production away from China to other countries.

However, these measures carry steep costs, which help further explain why, across industry, the top strategy was strengthening relationships with existing critical suppliers, since it requires less financial investment. This was equally true for government agencies. The bureaucratic processes, due diligence, and transparency requirements often associated with government procurement create a strong incentive to maintain and strengthen established relationships. Government agencies often prefer to reinforce their ties with incumbent contractors and suppliers that have a proven track record and are already attuned to the specific regulatory and compliance requirements typical of public sector engagements.

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.

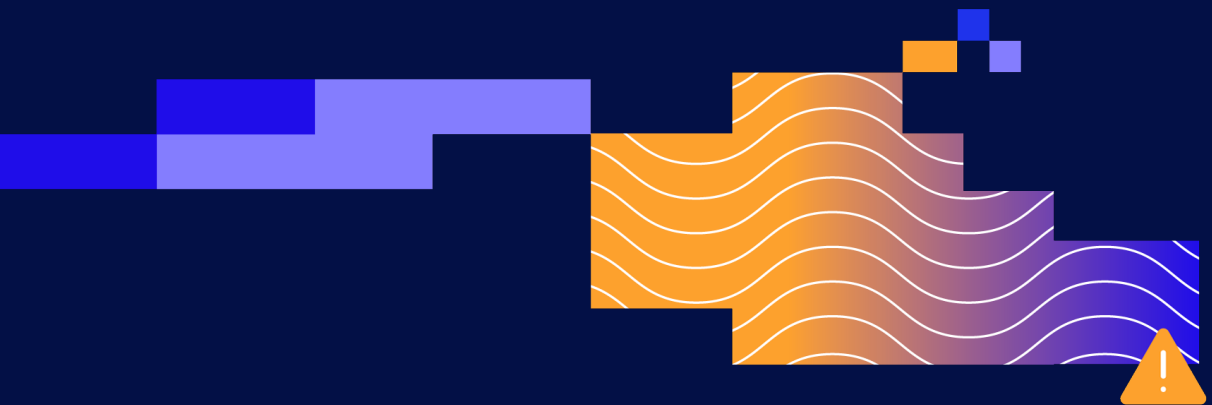
SECTION 02

The State of Supply Chain and Third-Party Risk Management

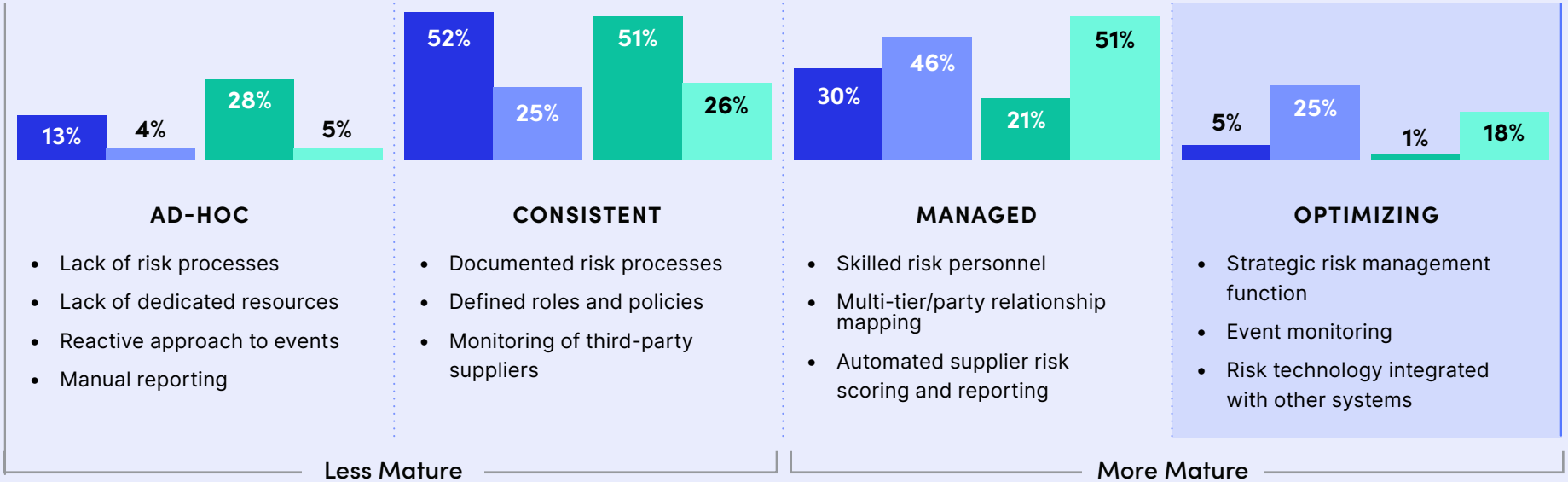
Maturity Set to Increase in Next Three Years

Despite major global supplier shocks in recent years, many government organizations still lack the visibility, resources, processes and tools needed to manage and respond supply chain risks at speed and scale. When presented with a four-stage model for SCRM/TPRM capability maturity, almost all (99%) of surveyed executives within government do not think they have reached the final stage of SCRM/TPRM maturity (see next page).

Additionally, over three quarters (79%) of government organizations self-identify at a lower level of maturity today – specifically, as “ad-hoc” or “consistent” on the Interos SCRM/TPRM maturity scale – compared with just 21% who rate themselves as more mature – defined as “managed” or “optimizing”.



Interos SCRM/TPRM Maturity Scale



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

Industry Average
- Today
- In the next 3 years

Government Average
- Today
- In the next 3 years

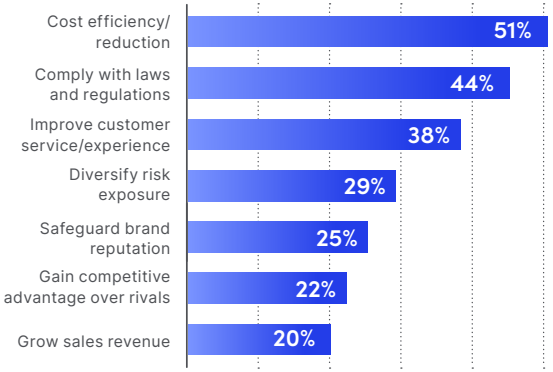
This changes dramatically when asked where they expect to be in three years, with 69% of government respondents expecting to be at the mature end of the spectrum characterized by the following capabilities:

- A standalone SCRM/TPRM function to proactively manage risk
- Skilled risk management personnel with codified and budgeted training programs
- Agreed processes and effective internal collaboration around these
- Multi-tier visibility of the extended physical and digital supply base
- Automated supplier risk assessments and executive reporting
- Continuous monitoring of potentially disruptive events

Government organizations were more likely to use the lower half of the scale/rate their program as less mature today, than any other vertical surveyed – but expect to rise to meet the cross-industry average over the next three years. Clearly, government agencies expect to invest heavily in improving SCRM/TPRM in the immediate term.

> "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**, U.S.

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



Benefits of Enhanced SCRM: Cost Efficiency, Compliance, and Customer Service

The ambition to improve risk management practices is shared by all sectors. The data shows that within government organizations, increasing cost efficiency is the main business driver for improving SCRM/TPRM (51%). This contrasts with the cross-industry results where improving customer service was the top priority by a slim margin (cost efficiency was still the second most-cited driver overall). The difference here reflects increasingly tight federal budgets and the comparatively high degree of oversight and public accountability within the federal procurement process. Agencies were also 10% more likely than the average to be motivated by regulatory compliance.

The contrast was sharpest between government agencies and respondents from the Aerospace & Defense (A&D) sector. In most other questions within our survey, A&D and government respondents had similar answers – but in this instance A&D organizations were half as likely as government respondents to count cost-efficiency as a motivator of SCRM/TPRM implementation. The disparity may indicate that A&D organizations see themselves as having already achieved the greater cost efficiency that government organizations lack. It may also reflect the fact that within Aerospace & Defense innovation, agility, and technological differentiation are key to success – compared to government organizations' focus on responsible stewardship of tax dollars and mission-readiness.

Better Risk Management Has Financial Benefits

Government participants, when asked to quantify the value of improved risk management expected to save an average of $26 million annually – almost half (48%) of their average annual losses from disruption ($54M).

As with maturity, government organizations' responses indicated some pessimism or reduced expectations when compared to commercial organizations. This was another area where they contrasted sharply with private A&D respondents, who were the most optimistic about the potential financial benefits of better TPRM/SCRM – and expected that they would recover $47M on average (or ~3/4 of the cost of supply chain disruption).

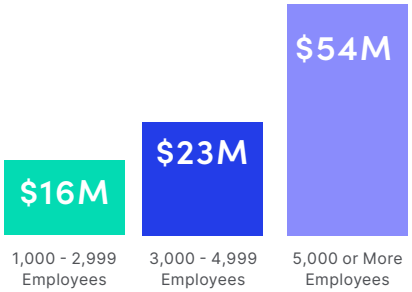
It is also worth noting that government leaders' expectations for the financial benefit of faster reactions times/better planning scaled with organization size. Larger government agencies (those employing 5,000 or more people) expected to recoup $54M annually, while smaller organizations (those with 1,000 to 2,999 employees) expected a $16M financial benefit, on average.

Similarly, government organizations that lost more of their budget due to supply chain disruption also estimated that greater preparedness would save them larger sums than organizations that lost less. For example, agencies reporting losses between $100M - $250M thought better preparedness would save them $40M annually, while organizations that lost between $1M -$10M estimated $9M in savings from improved SCRM. These findings indicate that government leaders believe the financial benefits of better preparedness and faster response times to be highly scalable.

> "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,** U.S.

$26M

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



Annual estimated **savings from increased preparedness** for smaller vs larger government organizations

"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, U.S.

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

1. Lack of visibility into sub-tiers of our extended supply chain. **46%**
2. Lack of reliable data to inform goal-setting and progress tracking. **41%**
3. Lack of financial resources/ investment budgets. **40%**

Government Leaders Split on ESG's Importance

Just one quarter (25%) of our government 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. So it is unsurprising that, given the reduced interest in brand protection, only 18% of government leaders said they are stepping up ESG supply chain activities and investments – compared to 47% for financial services, 40% for healthcare, 36% for A&D, and 34% for energy.

More than half (61%) of government procurement leaders acknowledge that their ESG efforts have taken a backseat for the time being. They recognize the issue's importance but managing costs and supply availability currently supersede ESG activities in their organizations.

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

- Carbon Emissions
- Renewable Energy
- Recycling and reuse of materials

The area where government organizations say they've made the least progress is eradicating child labor from their supply chains, with only 45% of government leaders reporting moderate-to-significant progress. There were some differences in how government leaders on both sides of the Atlantic viewed their progress on ESG risk, with U.K. & Ireland government respondents almost half as likely to report progress in eliminating child labor, forced labor, and deforestation than their North American counterparts.

Core ESG Challenges: Usable Data, Sub-Tier Visibility

Despite the importance of ESG objectives to supply chain and third-party risk managers, significant challenges remain in pursuing ESG supplier improvements. In addition to competing priorities and budget constraints, a lack of reliable data and poor sub-tier visibility were also cited as barriers to ESG progress. All are critical in the ESG domain, where violations of environmental and social standards can often occur further upstream in supply chain networks where organizations have many indirect vendor connections.

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**	**80%**
These laws compel our organization to improve our supply chain/ third-party risk management capabilities and **invest in new processes, people and/or technology**	**85%**
New regulatory requirements force us to improve our awareness of critical **indirect (e.g., tier-2/3 or fourth/fifth party) suppliers**	**81%**

Regulations Promote Better Risk Management

Complying with a growing body of laws and regulations is a fundamental part of supply chain risk management for most organizations, as it is with cybersecurity and broader operational resilience programs. Government organizations were also more likely to list compliance as a main business driver for implementing SCRM/TPRM than any other industry we surveyed.

More than three-quarters (79%) of government leaders agree that legislation imposes "a heavy burden" on their organizations from a cost, time, data and resources standpoint. However, the findings show it also spurs risk management capability development.

A slightly higher percentage (85%) say that new laws compel them to invest in risk processes, people and technology – and 80% agree this investment in technology is critical to ensure compliance. Six out of 10 go further than basic compliance, welcoming stricter laws on the grounds they are an opportunity to gain a competitive advantage against rivals.

Regulations Promote Collaboration and Awareness

Six out of 10 government procurement heads believe that regulations force them to improve collaboration 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 internally and externally, was identified as a key improvement priority in the **2022 Resilience report**.

Cyber, ESG and other laws also force organizations to improve visibility of direct and indirect suppliers, according to 81% of government survey participants. This is an essential foundation for maturing SCRM/TPRM capabilities and driving greater operational resilience.

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 supplier ecosystems and understand key dependencies and relationships at multiple tiers

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

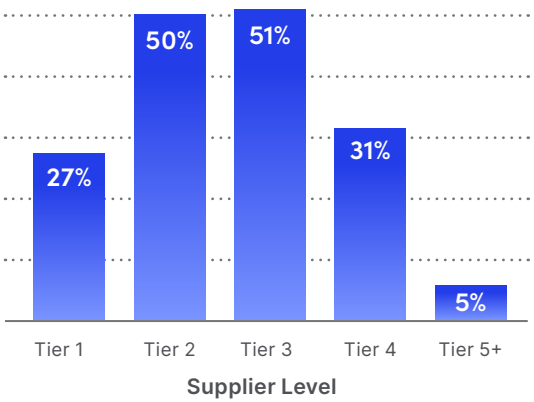
3. **Monitor** events across their global networks in real time or near real time, so they can react quickly when required

Mapping, modeling and monitoring are important parts of an ecosystem-based approach to supply chain risk management. They are designed to identify issues and potential sources of disruption earlier so that prompt mitigating actions can be taken.

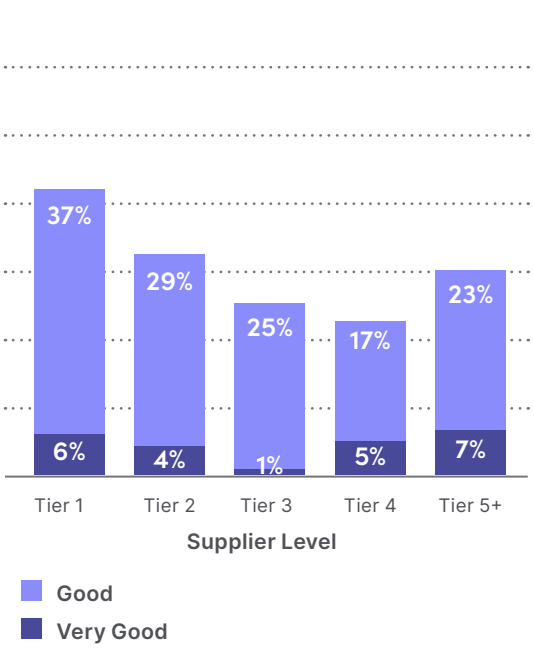
How Interos Defines Operational Resilience

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.

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.

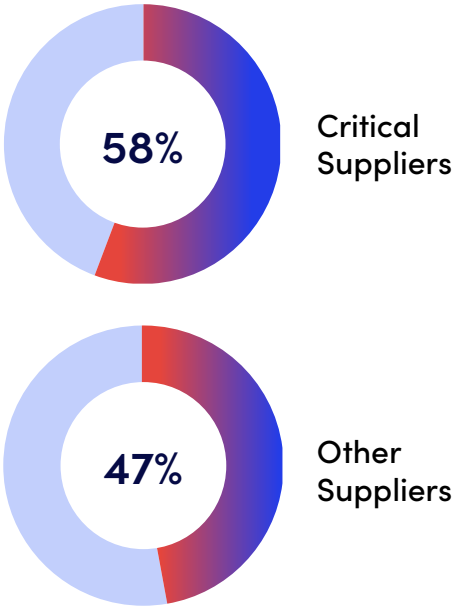
Disruptive supply chain events – whether a supplier bankruptcy, a factory fire, a cyber-attack, or another incident – often originate among sub-tier suppliers. Our survey data shows that in the past 12 months tier-3 suppliers were the most common source of disruption for government organizations, followed by those at tier-4 – which were only a single percentage point ahead of tier-3. These responses indicate that effective SCRM/TPRM programs must monitor relationships beyond tier-1 suppliers.

Government agencies have significant work to do here – reporting worse levels of visibility than any other industry surveyed. Even at tier 1, less than half (43%) of government agencies report "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 tier 2 that number fell to 33%, and at tier 3 only a quarter of respondents (26%) believed they had this degree of information.

Government respondents estimated lower levels of visibility to those in the A&D, financial services, healthcare, and energy industries across tiers 1 and 2. At tiers 3 and 4 they remained below the average but slightly ahead of healthcare. There is clearly room for widespread improvement here. Within government, visibility varied greatly by SCRM program maturity, with more-mature organizations more likely to report good/very good visibility at tiers 2-5+ than their less-mature counterparts.

> "Use technology tools to enhance visibility and transparency in the supply chain and third-party relationships."
>
> **– Procurement Leader,** 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 sub-tier relationships and dependencies is an essential step in determining where weaknesses and vulnerabilities exist that may need to be addressed through mitigation strategies. But government organizations also need 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 essential to business units, provide critical products and services, have good strategic fit with their customer, and so on – and "other" suppliers. Within government, only 58% of critical suppliers and 47% of other suppliers are subjected to a risk assessment during the sourcing and supplier management process, on average.

These 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,** 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 risk management. But in a dynamic, fast-changing risk landscape, these periodic interventions are not sufficient to anticipate disruptive events. Organizations need continuous monitoring across their extended supply chains to achieve this.

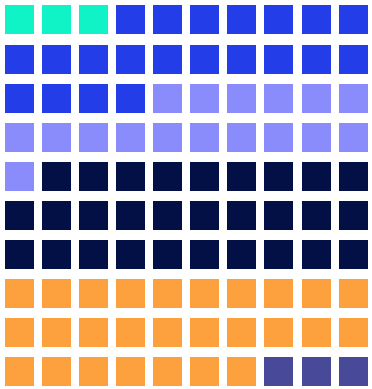
Just 3% of government procurement leaders say they monitor their most critical suppliers daily, with 21% indicating weekly (more mature organizations are slightly higher on both frequencies). Just under half (46%) conduct risk monitoring on a quarterly or biannual basis. For other suppliers, the frequencies are lower still, with 25% saying they only assess non-critical suppliers on an ad-hoc basis/when a problem arises. On average, government organizations assess critical suppliers every 25 weeks – less frequently than the cross-industry average of 20, and less often than any other industry. However, they assess "other" suppliers every 24 weeks (a little more frequently than the cross-industry average of 26). This leaves organizations vulnerable to unexpected and unpredictable risk events.

Notably, government organizations that report positive economic expectations for the year assessed critical suppliers much more frequently (every 18 weeks) compared to those with negative expectations for the year (every 32 weeks), indicating that organizations with better insight feel more confident in their economic performance.

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

– Procurement Leader, U.K. & Ireland

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

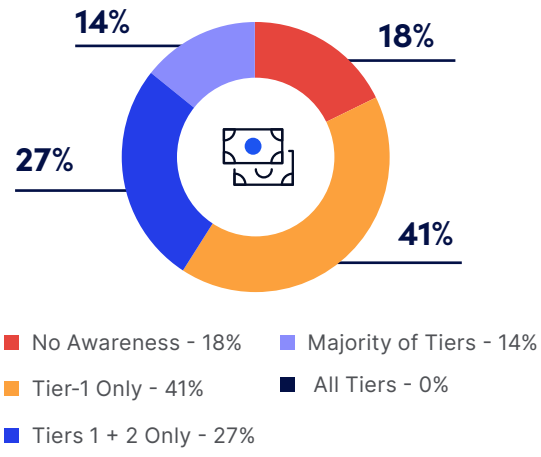


- Daily - **3%**
- Weekly - **21%**
- Quarterly - **17%**
- Every six months - **29%**
- Annually - **27%**
- Ad Hoc - **3%**
- Never/Don't know - **0%**

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	1%
...becomes financially insolvent	0%
...disrupted by a geopolitical issue	1%
...experiences an operational disruption	1%
...disrupted by extreme weather/natural catastrophe	1%
...becomes the subject of a restriction/ sanction	3%

Government Awareness of Supplier Financial Insolvency within 48 Hours



4. Risk Event Awareness Requires Improvement

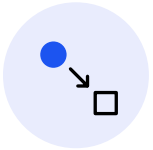
Early awareness and notification of third-party risk events at different supply chain tiers is vital for customer organizations to appropriately respond and mitigate limit any negative impacts. The first few days after an incident are a critical window for assessing the situation and taking action. This includes activating contingency manufacturing plans, mobilizing rapid-response engineering teams, reallocating strategic inventory reserves, initiating alternative supplier engagements, and implementing enhanced security protocols to safeguard sensitive information and technologies.

3% or less of government procurement leaders say they are aware of various risk events within 48 hours of occurrence across every tier of their supply chain. Between 43% to 62% of our government sample (depending on the type of risk event) would have either no visibility of a third-party risk event – cyber-attack, ESG violation, insolvency, etc. – within 48 hours or only have visibility at the tier-1 level – so significant improvements are needed here.

A further one-third of our government sample believe they would be aware of events at tiers 1 and 2 within 48 hours, but not tiers 3, 4 or 5.

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

36%
People



34%
Processes

39%
Technology

5. Invest in Risk People, Processes and Technology

Improving SCRM and TPRM capabilities demands a mixture of people, process, and technology. Given recent economic and political turmoil particularly over federal budgets within the U.S., it makes sense that government leaders have less optimism about 2023 as whole. Only 51% of government respondents were positive about their organization's financial outlook for the year. Compare that to the cross-industry average where 82% expressed a positive outlook.

This relative pessimism translates into expectations about the resources they are likely to have to manage risk. Only a minority (34% - 39%) expect to grow their investments in people, process, and technology this year. Compare that to the cross-industry average, where a majority expect to increase these investments. Between 25% - 38% of government respondents say spending will be flat in each of the three areas (a greater percentage than any other vertical). Government agencies were also more than twice as likely than any other industry to report a decline in investment in people – a sign of where tightening federal budgets will make their impact.

Government organizations that reported greater SCRM program maturity were twice as likely as less mature organizations to say they are significantly increasing their investments in technology this year.

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

Top three benefits of SCRM and TPRM technology solutions

Ability to identify high risk suppliers across multiple factors

Data/analytical support for risk mitigation

Visibility of multi-tier supplier relationships/ dependencies

"We use advanced data analytics, allowing us to take fast action and make decisions based on events as they happen."

– Procurement Leader, US

Top Tech Benefits: Risk Spotting, Decision Support

Government executives consider the three greatest operational benefits of SCRM and TPRM technology solutions to be data/analytical support for risk mitigation actions, visibility of multi-tier supplier relationships/ dependencies, and the ability to identify high-risk suppliers across multiple factors. But just four percentage points separate these benefits from others that respondents ranked among their top three – namely, speeding up due diligence during supplier selection, improved executive reporting, and rapid notification of risk events and potential disruptions.

No respondent, in government or across every vertical surveyed, said they saw no benefits to investing in a SCRM/TPRM technology solution.

From a maturity standpoint, government organizations with less mature SCRM programs were more likely to value the ability to identify high risk suppliers across multiple factors, and less likely to see merit in the rapid notification of risk events and potential disruptions than their more mature counterparts. This may indicate that more mature organizations feel they already have a handle on their suppliers' broader risk profiles and see faster awareness of disruption as the next major frontier of advancement.

SECTION 04

Recommendations to Build and Sustain Resilience

- **Invest in continuous, multi-tier supply chain risk visibility.** Only 3% of government procurement organizations continuously monitor their suppliers, and roughly two-thirds lack good visibility of all tiers within their supply chains. Without this level of insight, agencies are relying on lagging point-in-time snapshots that leave them vulnerable to disruption and falling behind the commercial sector who are seizing the advantage comprehensive visibility provides.
- **Apply and track progress against a maturity model.** More mature organizations have lower costs associated with disruption – yet 99% of government organizations think they need to improve their risk management capabilities. To start realizing these benefits, organizations need to establish performance baselines for progress comparison, document processes, and invest in strategic risk functions, skilled personnel, and risk technologies that integrate 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 disruptive events strike. Currently, far too many government organizations don't know about a supplier disruption in the first 48 hours, leaving them flat footed in a stakeholder environment that demands rigorous, responsible, and ethical corporate responses. By investing in resilience, organizations can increase the scope of disaster recovery activities to include their third parties - bridging the gap between procurement and operational resilience teams.

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

- **Forge internal collaboration between risk owners and functions.** Supplier risk management accountability may rest most often with the procurement function (and does for 21% of our government survey sample), but ESG, cyber, financial and other risks are often jointly owned. Alignment and collaboration between procurement and other 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. In fact, it was the top resilience strategy selected by government survey participants. This first requires identifying who those critical partners are. Then sharing information on multi-factor risks and in some cases, making shared investments to mitigate the most critical of them. Shared technology solutions that enable risk visibility can greatly aid this process. 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 via spreadsheets. Advanced software and data analytical capabilities are essential for identifying, assessing, mitigating, and monitoring multi-tier supply chain risks on a continuous basis. 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 AI-first operational resilience company – helping clients achieve Resilience by Design™. Our pioneering scoring and relationship discovery technologies enable customers to automate risk assessment, detection, and response. As the world's first, and only, automated supplier resilience platform, we map and monitor physical and digital supply chains at scale to protect organizations from regulatory violations, unethical labor, cyber-attacks, bankruptcy, catastrophe, and other systemic vulnerabilities. Interos serves a variety of commercial, government, and public sector customers around the world including a host of Global Fortune 500 companies from within the members of the Five Eyes nations.

Learn More

Additional Information:
www.interos.ai or 1 (703) 745-5578

101723