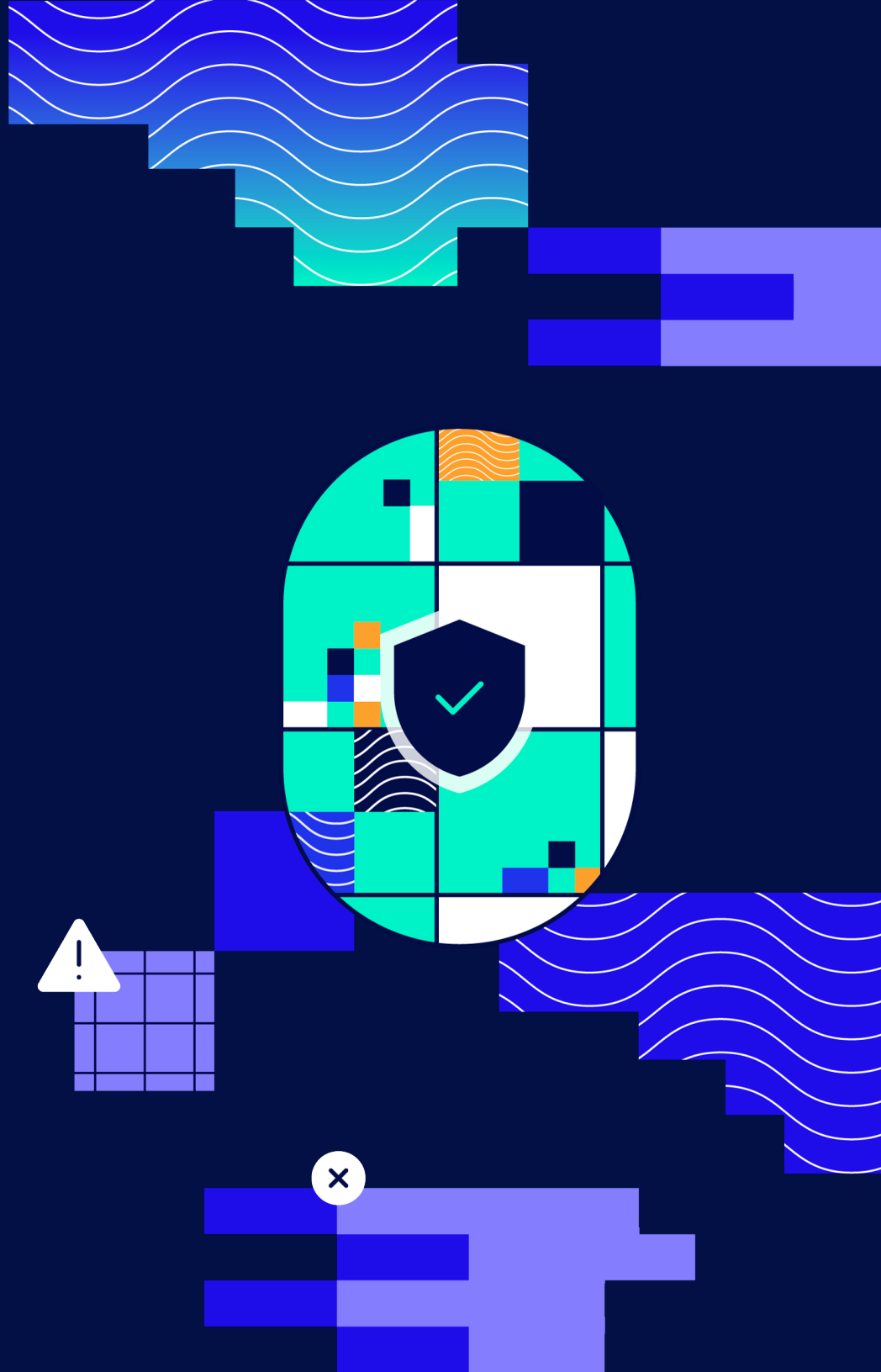
interos

THE THIRD ANNUAL INTEROS SUPPLY CHAIN SURVEY

Invisible Threats: Resilience 2023

Aerospace & Defense 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 aerospace and defense (A&D) organizations highlight an industry caught in the throes of turbulent economic forces. Organizations 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, damage, and loss.

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 today's complex and fast-moving enterprises remain unstoppable."

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 within the aerospace & defense industry (A&D) 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 gain a competitive advantage while safeguarding brand reputation – is driving A&D organizations to advance TPRM/SCRM maturity.

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

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

Key Findings

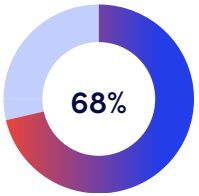
4

The average aerospace & defense organization experiences **four supply chain shocks** requiring "significant mitigating action" annually

↑ $47M

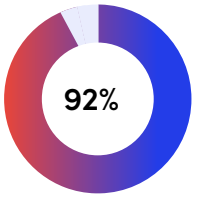
A&D organizations believe they **can recover $47M annually** by preparing better for and reacting faster to disruption

RISK ASSESSMENT



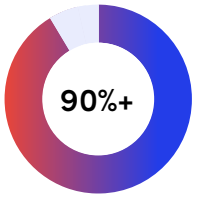
On average, A&D organizations only assess 68% of their critical suppliers for risk

RISK MANAGEMENT MATURITY



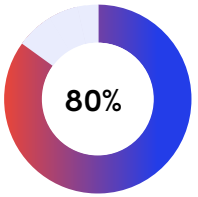
92% of A&D organizations do not consider themselves to have reached the highest level of SCRM/TPRM maturity

EVENT AWARENESS



90%+ of A&D 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

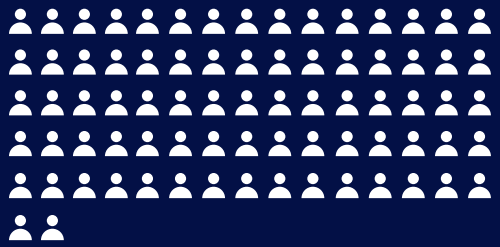


80% of aerospace & defense procurement leaders agree that they cannot comply with emerging regulations without supporting data, analytics, and risk management software

Out of the

150

Senior procurement leaders we surveyed...



77 are from the **United States**

47 are from the **UK and Ireland**

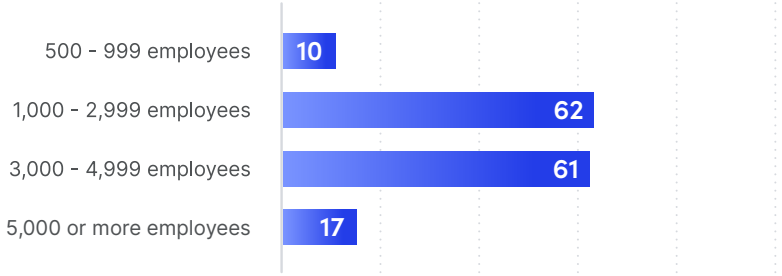
26 are from **Canada**

70 are within senior management

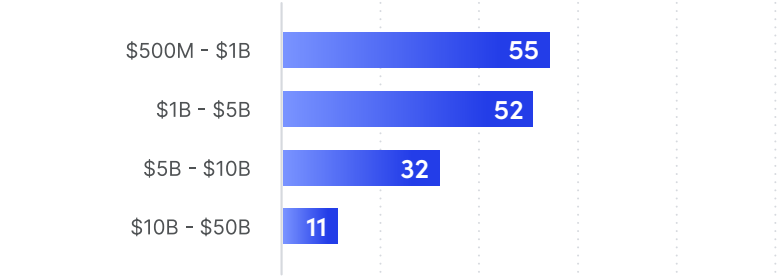
80 are C-level or board members

Demographics

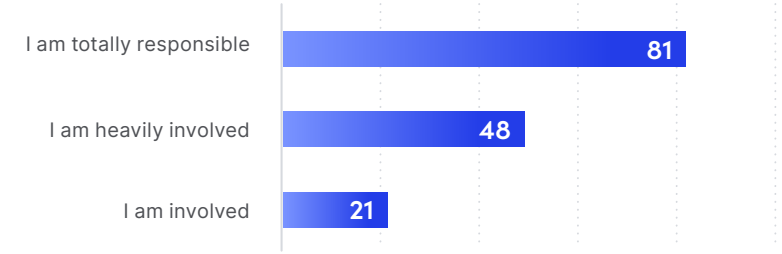
Q: How many employees does your organization have globally?



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

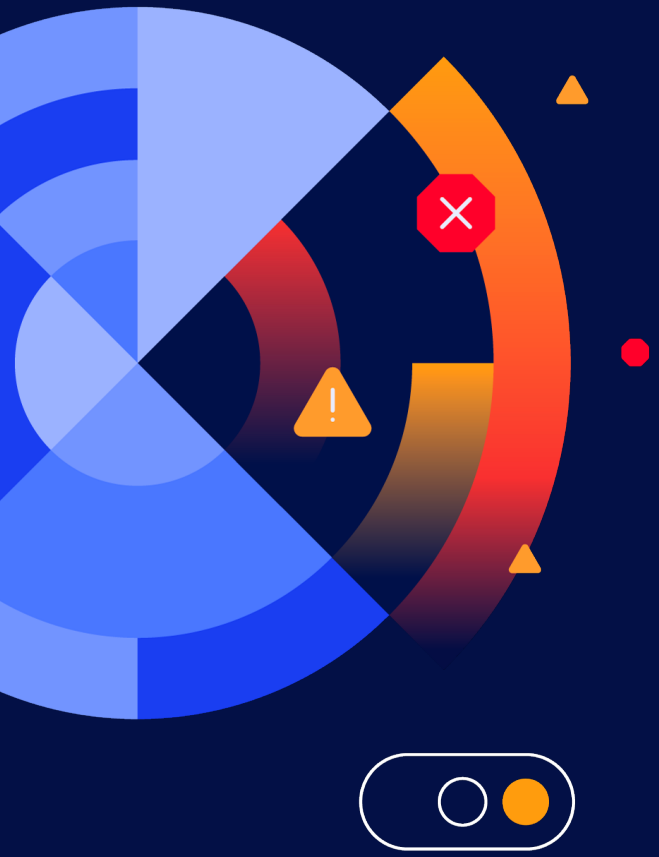


Q: What is your level of involvement when it comes to managing the global supply chain in your organization?



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 A&D organizations and their supply chains 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 $65M Gap

Supply chain disruptions are frequent and costly. In total, 150 A&D organizations participated in the study. On average each lost a total of $65M in revenue responding to four major supply chain disruptions within the past 12 months. These were events requiring "significant mitigating action." Mitigation included activating alternative suppliers, shifting production lines, utilizing buffer inventory or revising delivery schedules.

While the overall disruption costs for A&D organizations dropped in comparison to our 2022 survey, the number of significant supply chains disruptions increased, from three to four annually, a 33% jump.

> "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 **UP 33%**
FROM 2022

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

$65M

Annual financial impact as a result of these supply chain disruptions

$19M

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

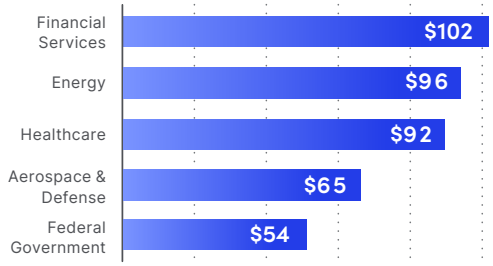
$80M

Average annual cost of disruption for A&D companies with $10B - $50B in annual revenue

$43M

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

Costs by Vertical (in USD millions)



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).

This disparity may reflect the fact that aerospace & defense, and government sectors often have more controlled, localized supply chains. They protect mission-critical supply chains with contingencies and stockpiles. These sectors are also less demand-sensitive, with demand driven by long-term contracts and federal policy, rather than immediate consumer need. Because they typically develop additional planning and alternative sourcing to absorb and manage disruptions, they are more likely to experience reduced financial impact when disruptions occur.

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 A&D organizations (those with between $500M - $1B in annual revenue) lost an average of ~6% ($43M) of that revenue to supply chain disruption. On the other end of the scale, larger organizations (those with between $10B - $50B in annual revenue) only lost ~3% ($80M) on average. The cost of disruption scales with the size of an organization – but not 1:1. While disruption is costly for orgs of all sizes, smaller organizations' generally lower levels of risk management maturity (detailed later in this report) may be responsible for the outsized impact of disruption to their bottom line.

> "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.

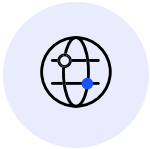
Q: What annual cost increases and/or revenue losses does your organization experience annually?

FINANCIAL

$39M

CATASTROPHIC

$49M



GEOPOLITICAL

$44M

CYBER

$36M

ESG

$38M

RESTRICTIONS

$44M

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 executives at aerospace & defense companies reported annual cost increases and/or revenue losses ranging from $36M to $49M 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

Catastrophic risks were the most expensive disruption for A&D firms, driven by a steadily increasing amount of costly natural disasters. Per NOAA, 2023 has already set records as the year with the most natural disasters that caused over $1B in damages. This contrasts with the cross-industry results where restrictions-related disruptions led the way. Given that many emerging restrictions were from Western governments targeting Russian and Chinese entities, the reduced impact to A&D firms is likely due to the fact that they were already largely barred from engaging with these nations.

The findings highlight that organizations cannot afford to disregard any type of individual 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 A&D firms put cyber attacks in their top 5 risks

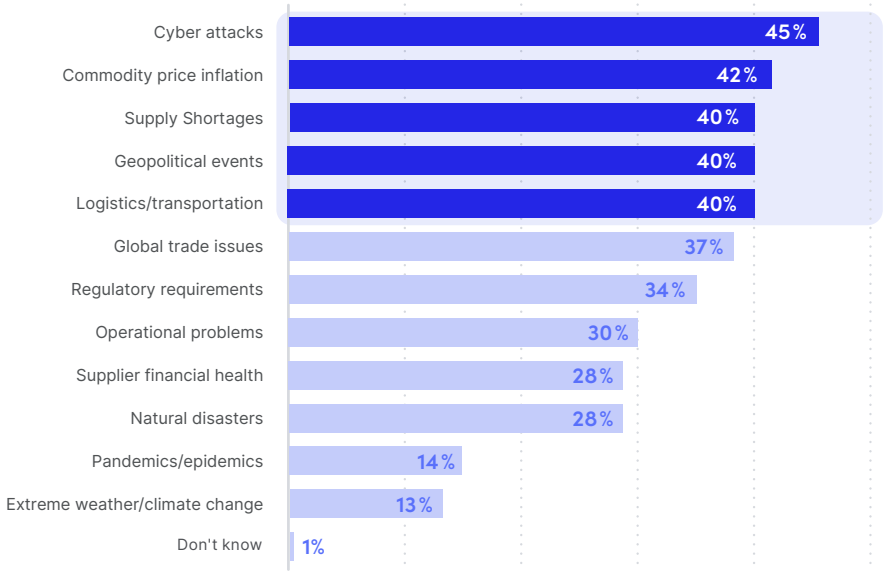
Top Crisis Triggers: Cyber-Attacks, Inflation

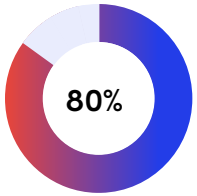
Cyber-attacks and commodity price inflation top the list of concerns for A&D procurement leaders by a slim margin. While A&D organizations are near-equally concerned about the array of threats that face, they are less concerned about certain issues such as pandemics, possibly reflecting that while events like COVID-19 can be incredibly disruptive, costly, and destructive – leaders feel that their ability to plan against them is limited.

A&D leaders were between 10% - 20% more likely to be concerned about the impact of supply shortages, inflation, cyber-attacks, and geopolitical events on their supply chains, than those in financial services, healthcare, and energy. A&D leaders were also more concerned about logistics issues than other verticals.

These elevated levels of concern reflect the criticality and sensitivity of the work of A&D and 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, and 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 A&D 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	49%
	Uyghur Forced Labor Prevention Act (UFLPA)	75%
	National Defense Authorization Act (NDAA) Sections 889/5949	71%
	Interagency Guidance on Third-Party Relationships – US	67%
	German Supply Chain Due Diligence Act	38%
	Digital Operational Resilience Act (DORA)	53%
	Corporate Sustainability Due Diligence Directive (CSDDD)	43%
	Critical Raw Materials Act – EU (proposed)	40%
	PRA/FCA Operational Resilience Regulations	51%

* 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 ESG, cybersecurity and operational resilience. A slew of others are also in the pipeline.

When asked about a variety of supply chain regulations, A&D organizations were generally less concerned over the issue than most of the industries we surveyed. Specifically, when it came to the six non-U.S.-related regulatory measures, A&D organizations were between 12% - 24% less likely than the cross-industry average to say that the regulations would have a significant/moderate impact on their business.

There were two regulations that A&D respondents did show equal or elevated levels of concern over: The first being Sections 889/5949 of the National Defense Authorization Act (NDAA). A&D's concern over NDAA requirements comes as no surprise, given that an overwhelming majority of A&D organizations have contracts with the U.S. government and must comply with NDAA provisions as a matter of course. Sections 889/5949 are part of the ever-tightening sourcing rules related to Chinese technology in U.S. federal government contracts (Section 889 and 5949).

The second regulation was the Uyghur Forced Labor Prevention Act (UFLPA). The UFLPA creates a presumption that all goods from the Xinjiang region of China are made with forced labor – and empowers border officials to seize all shipments of products suspected of being made there. A&D organizations are right to be concerned about this law given that they often have extensive, complex supply chains that may include raw materials mined or processed in Xinjiang without their knowledge.

80% of A&D 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. The majority of A&D respondents consider legislation helpful in forcing organizations to improve supply chain and third-party risk management capabilities, as do 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, 91% of A&D participants say they are "extremely" or "somewhat" concerned – a higher percentage than any other vertical.

Difficulties in getting essential raw materials/components are uppermost in A&D CPO's minds. They are also concerned about the potential for losses in cost efficiency due to geopolitical disruption but are similarly worried about increases in costs stemming from resilience-building measures intended to counter disruption, such as inventory build-up and supplier diversification. Clearly, A&D leaders will need to carefully balance the up-front costs of resilience against potential efficiency losses.

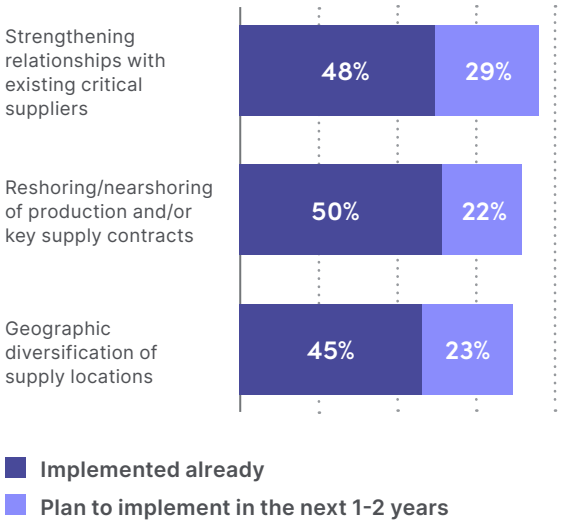
91%

of A&D 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. Damage to cost efficiency from resilience-building measures
3. Cost increases as a direct result of geopolitical events

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



Better Relationships, Reshoring, and Diversifying Key to Resilience

A&D organizations have restructured their global supply chains and supplier networks in response to geopolitical risk events. A majority of A&D firms (as well as organizations across industry) have met this challenge by reshoring or nearshoring key supply contracts and diversifying global footprints. 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 strategy was most popular within A&D, reflecting the specialized nature of A&D components, which often require rigorous quality controls, certifications, and security measures. Additionally, A&D supplier relationships are exceptionally strategic. Replacing or adding new suppliers isn't as simple as in some other industries, due to qualification requirements. These relationships are also crucial for managing complex regulations and compliance requirements that are inherent in the defense sector.

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.

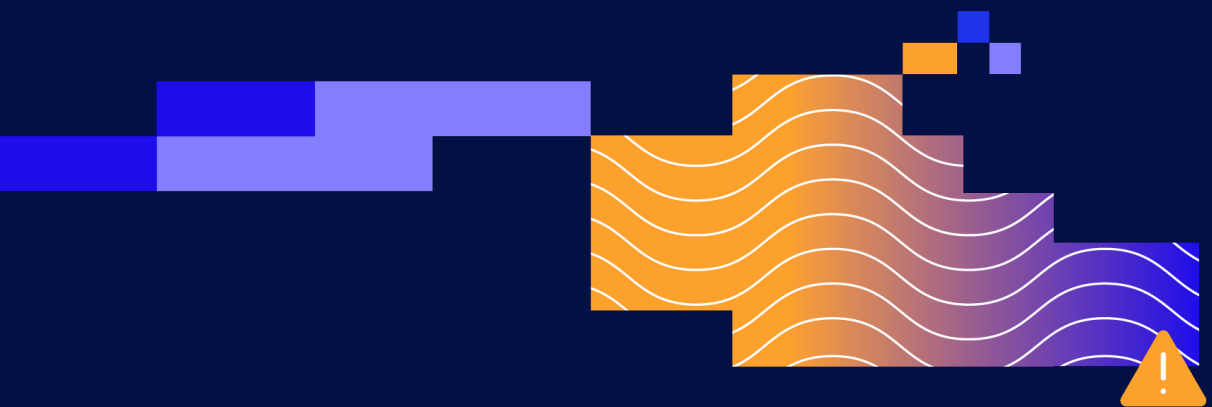
SECTION 02

The State of Supply Chain and Third-Party Risk Management

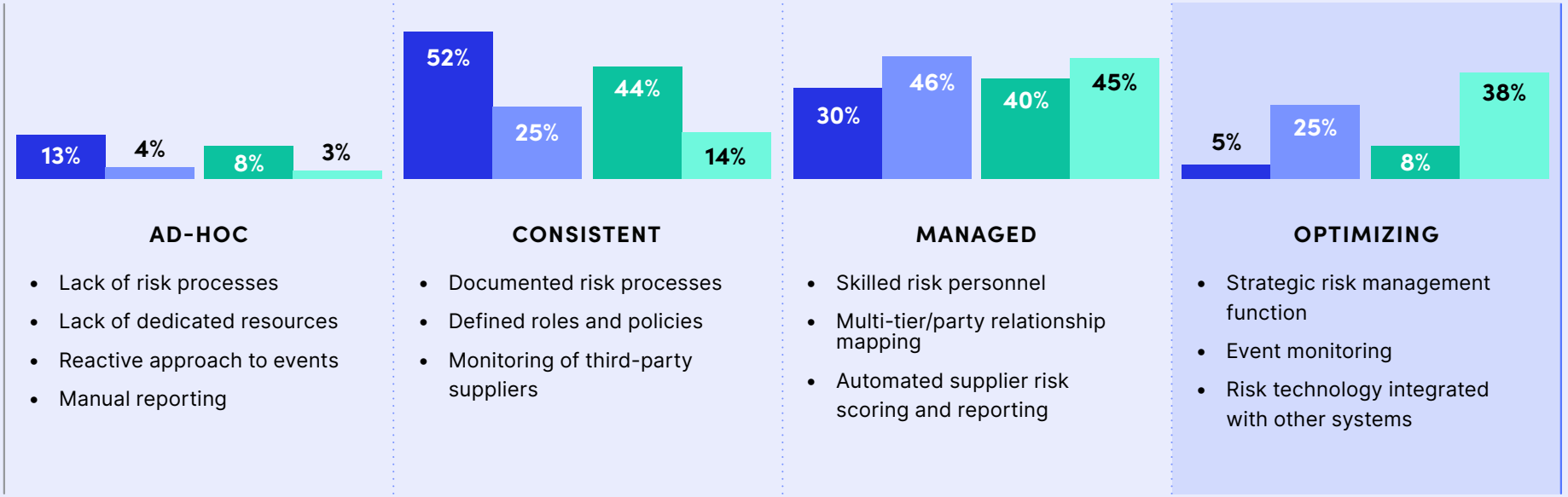
Maturity Set to Increase in Next Three Years

Despite major global supplier shocks in recent years, many aerospace & defense 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, an overwhelming majority (92%) of surveyed executives within aerospace & defense do not think they have reached the final stage of SCRM/TPRM maturity (see next page).

Additionally, slightly more than half of A&D organizations (52%) self-identify at a lower level of maturity today – specifically, as “ad-hoc” or “consistent” on the Interos SCRM/TPRM maturity scale – compared with slightly less than half (48%) 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

A&D Average
- Today
- In the next 3 years

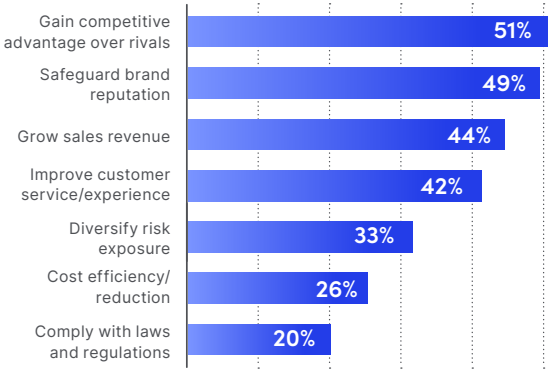
This changes dramatically when asked where they expect to be in three years, with 83% of A&D respondents (more than any other industry surveyed) expecting to be at the mature end of the spectrum characterized by the following capabilities:

- 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

"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: Competitive Edge, Brand Reputation, Revenue Growth

The ambition to improve risk management practices is shared by all sectors. The data shows that within A&D, gaining a competitive advantage over rivals is the most common business driver for improving SCRM/TPRM (51%). This contrasts with the cross-industry results where improving customer service was the top priority. The difference here reflects A&D's high-stakes contracts, where an organizations success or failure may hinge on a handful of contracts competed every few years – making securing a competitive advantage (alongside protecting brand reputation and growing revenue) through enhanced risk management much greater drivers.

A&D was also much less motivated by gains in cost efficiency than the cross-industry average, where it was the second-most-cited driver (26% in A&D vs 39% across industry). The reduced priority may indicate that A&D organizations see themselves as having already achieved greater cost efficiency. It may also reflect the fact that within Aerospace & Defense innovation, agility, and technological differentiation are key to success. While cost efficiency is important, given the strategic nature of most A&D work, the focus might be more on effectiveness, reliability, and risk management.

This may also reflect that A&D programs often take place over years and must evolve their project scope to adapt to changing circumstances – inflating costs over time.

Better Risk Management Has Financial Benefits

Aerospace & defense participants, when asked to quantify the value of improved risk management, expected to save an average of $47 million annually – almost three-quarters of their average annual losses from disruption ($65M).This includes both cost savings and higher sales.

As with maturity, A&D respondents led the way in optimism about the potential financial benefits of SCRM/TPRM. They are substantially more optimistic than government organizations, who were the least hopeful ($26M).

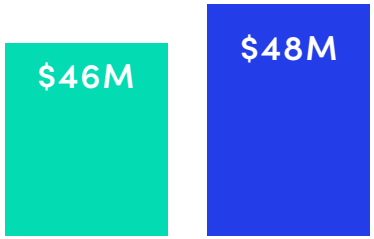
It is also worth noting that while those leaders who identify as more mature today estimate a slightly lower figure of $46 million in savings (compared to $48 million for their less mature peers). More mature A&D organizations also reported lower annual average costs of disruption ($57M vs $78M) So, A&D organizations experience lower disruption costs with higher levels of risk management maturity and, despite any additional running costs of SCRM/TPRM programs, achieve a better overall financial equation.

A&D organizations that lost more due to supply chain disruption also estimated that greater preparedness would save them larger sums (than organizations that lost less) – indicating that A&D leaders believe the financial benefits 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.

$47M

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 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, 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 extended supply chain — **47%**
2. Lack of reliable data to inform goal-setting and progress tracking — **43%**
3. Procurement organization has more pressing priorities — **41%**

A&D Leaders Split on ESG's Importance

Almost half (49%) of our A&D 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. More than one-third (36%) say they are stepping up ESG supply chain activities and investments – compared to 47% for financial services, 40% for healthcare, 34% for energy, and only 18% for government.

Just under half (48%) of A&D 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.

The following ESG areas are where at least 75% of A&D respondents say they've made moderate-to-significant progress in ESG supply chain risk management over the past three years:

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

The area where A&D organizations say they've made the least progress is deforestation, with only 35% of A&D leaders reporting moderate-significant progress.

Core ESG Challenges: Usable Data, Sub-Tier Visibility

Despite the importance of ESG objectives to A&D organizations and 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	**76%**
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**	**75%**
New regulatory requirements force us to improve our awareness of critical **indirect (e.g., tier-2/3 or fourth/fifth party) suppliers**	**73%**

Regulations Promote Better Risk Management

Complying with a growing body of laws and regulations is a fundamental part of ESG risk management for most organizations, as it is with cybersecurity and broader operational resilience programs. However, A&D organizations were largely less-concerned with compliance issues than other verticals, and were less likely to consider it a business driver for implementing SCRM.

More than three-quarters (76%) of A&D 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.

An almost identical percentage (75%) say that new laws compel them to invest in risk processes, people and technology – and 74% agree this 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

Seven out of 10 A&D 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 73% of A&D 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

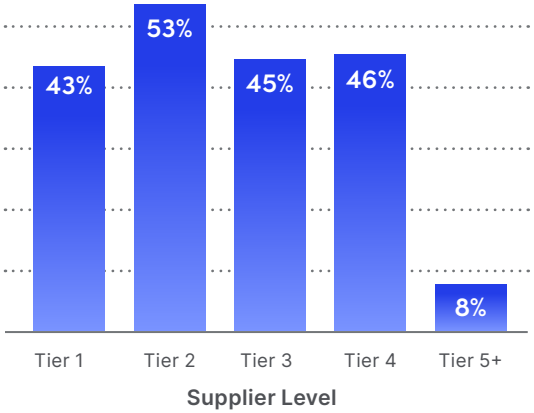
3. **Monitor** events across their global networks in real time or near real time, so they can react quickly when required

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.

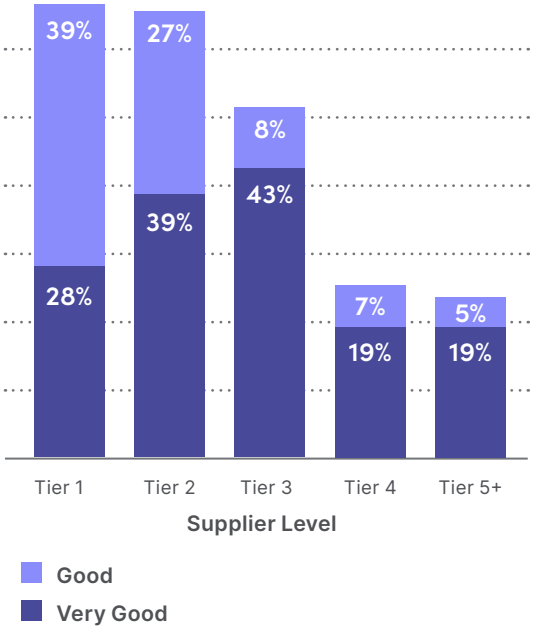
How Interos Defines Operational Resilience

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.

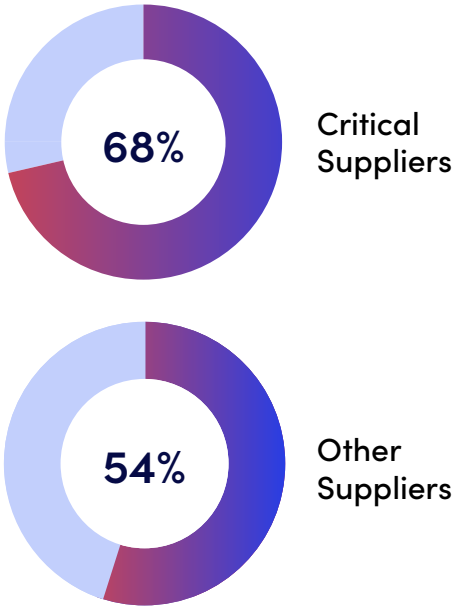
Disruptive supply chain events – whether a supplier bankruptcy, a factory fire, a cyber-attack, or another incident – often originate among sub-tier suppliers. Our survey data shows that in the past 12 months tier-2 suppliers were the most common source of disruption for A&D organizations, followed by 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.

Aerospace & defense companies have significant work to do here (though perhaps less than other industries surveyed). When asked about visibility levels at tier 2, two-thirds (66%) of A&D executives expressed confidence 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 tier 3, about half (51%) believed they had this degree of information.

A&D respondents estimated higher levels of visibility to those in the financial services, healthcare, government, and energy industries across tiers 1-3. They fell back in line with other sectors only at tiers 4 and 5+. Despite leading the pack, there is still clearly room for widespread improvement given that 34% of A&D firms still report moderate to low visibility at tier 1. Within A&D, visibility varied greatly by organization size, with larger organizations enjoying much greater visibility at tiers 1-3 than their smaller 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 A&D 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 A&D only 68% of critical suppliers and 54% of other suppliers are subjected to a risk assessment during the sourcing and supplier management process, on average. This was higher than any other industry.

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,** 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 cyber-security) 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.

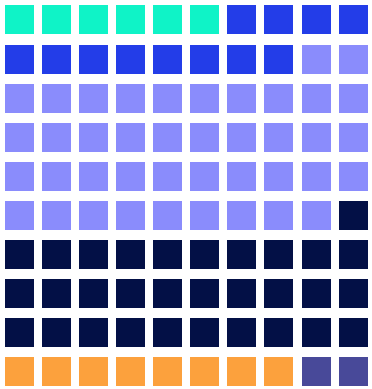
Just 6% of A&D procurement leaders say they monitor their most critical suppliers daily, with 12% indicating weekly (more mature organizations are slightly higher on both frequencies). Almost three-quarters (72%) conduct risk monitoring on a quarterly or biannual basis. For other (non-critical) suppliers, the frequencies are lower still, with 8% saying they only do this once a year. On average, A&D organizations assess critical suppliers every 18 weeks - more frequently than the cross-industry average of 20. However, A&D organizations assess "other" suppliers every 31 weeks (less frequently than the cross-industry average of 26 and the least-frequent of any industry). This leaves organizations vulnerable to unexpected and unpredictable risk events.

Notably, A&D organizations that report positive economic expectations for 2023 assessed critical suppliers much more frequently (every 17 weeks) compared to those with negative expectations for the year (every 24 weeks), indicating 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?

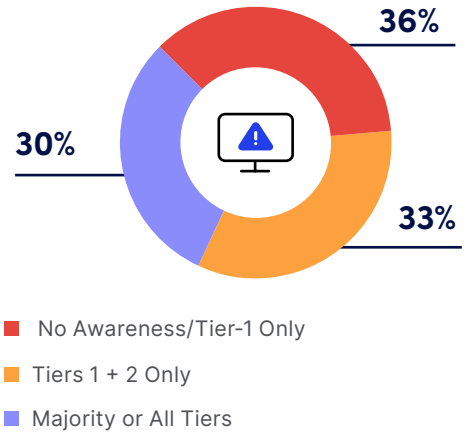


- Daily - **6%**
- Weekly - **12%**
- Quarterly - **41%**
- Every six months - **31%**
- Annually - **8%**
- Ad Hoc - **2%**
- Never - **0%**

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	7%
...disrupted by a geopolitical issue	5%
...experiences an operational disruption	5%
...disrupted by extreme weather/natural catastrophe	10%
...becomes the subject of a restriction/ sanction	4%

A&D Awareness of Cyber Attacks 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.

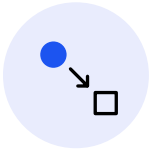
Less than 10% of A&D procurement leaders say they are aware of various risk events within 48 hours of occurrence across every tier of their supply chain. Between one-third to half of our A&D sample (depending on the type of risk event) would have either no visibility of a third-party risk event – cyber-attack, 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 A&D sample believe they would be aware of events at tiers 1 and 2 within 48 hours, but not tiers 3, 4 or 5.

Supply chain risk management maturity again plays a role. More mature SCRM/TPRM organizations were twice as likely to say that they would have 48-hour notification of financial insolvency at every tier of their supply chains than those that are less mature today.

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

55%
People



61%
Processes

62%
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 challenging economic environment, procurement leaders within A&D are generally optimistic about the remainder of 2023, with 86% positive about their organizations' financial outlook (in contrast with 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 16% and 27% say spending will be flat in each of the three areas.

More mature A&D organizations are 55% more likely to say they are significantly increasing their investments in technology this year, as they are with both people and process – though mature organizations preferred technology investment to a greater degree.

> "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

Enrich or speed up due diligence

"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

A&D executives consider the two greatest operational benefits of SCRM and TPRM technology solutions to be the ability to identify high-risk suppliers across multiple factors and data/analytical support for risk mitigation actions. But just 11 percentage points separate these benefits from others that respondents ranked among their top three – namely, speeding up due diligence during supplier selection, providing visibility of multi-tier supplier relationships and dependencies, and rapid notification of risk events and potential disruptions.

From an industry vantage point, A&D leaders were more likely than their peers in other industries to consider the ability to identify high-risk suppliers across multiple factors the key benefit of technology. This makes sense given the strategic importance of A&D products, stringent regulatory requirements, and their often-sprawling, global supply chains – all of which can amplify the impact of a supplier failure or increase the likelihood of risk events.

SECTION 04

Recommendations to Build and Sustain Resilience

- **Invest in continuous, multi-tier supply chain risk visibility.** Only 6% of A&D companies continuously monitor their suppliers, and most lack good visibility of all tiers within their supply chains. Without this level of insight, companies are relying on lagging point-in-time snapshots that leave them vulnerable to disruption and falling behind competitors 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 92% of A&D companies 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 A&D 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 23% of our A&D 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. In fact, it was the top resilience strategy selected by A&D 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. It is not surprising that most A&D 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 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

100223