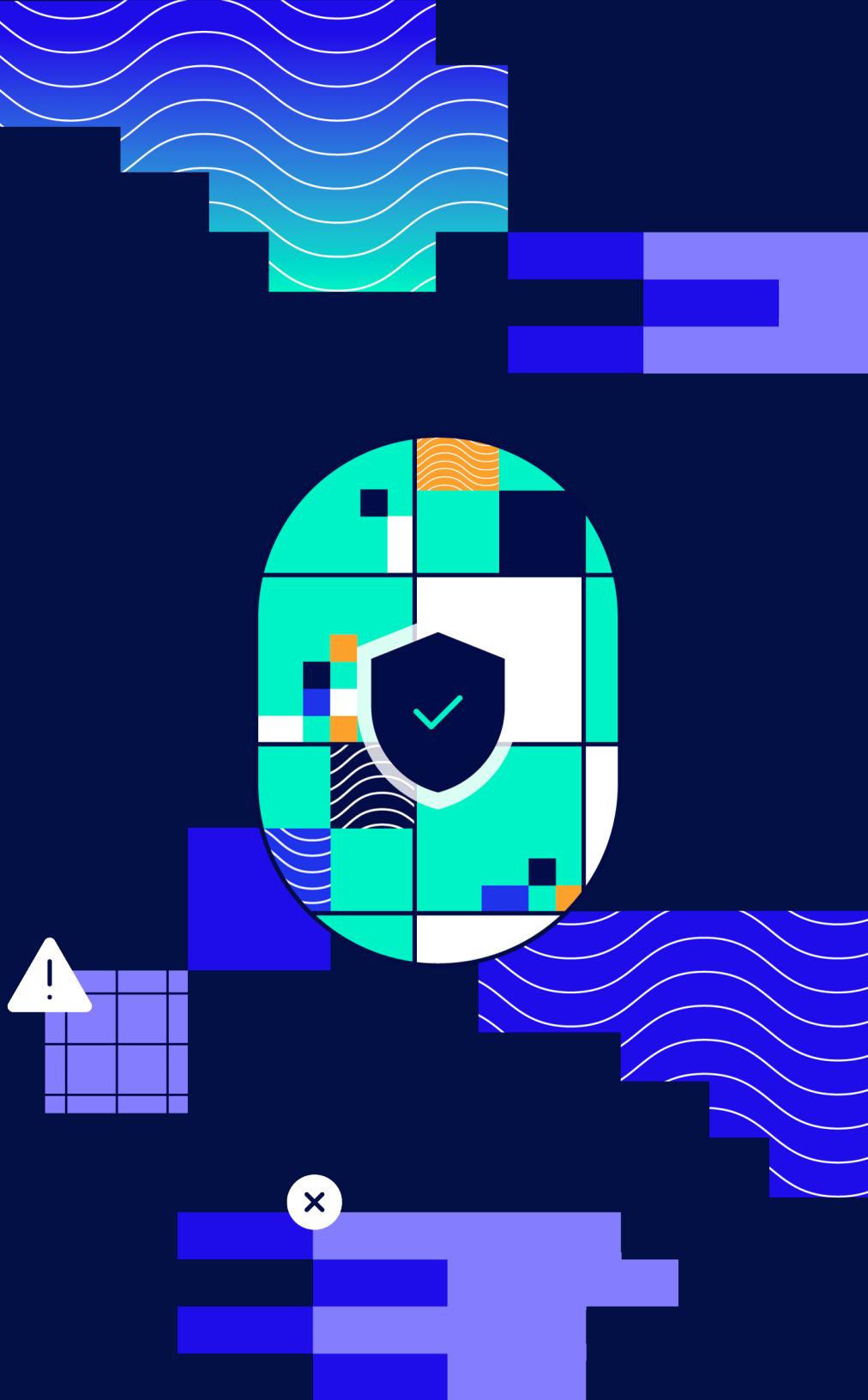
interos

THE THIRD ANNUAL INTEROS SUPPLY CHAIN SURVEY

Invisible Threats: Resilience 2023

Financial Services 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™. We developed this annual resilience benchmark to assist organizations in their journey toward this goal. Created by independent researchers with no mention of Interos, it’s the only industry report to quantify the impact of multifactor risk on global supply chains.

This year’s results for financial services organizations (FSIs) highlight an industry caught in the throes of a turbulent economic forces. Organizations continue to wrestle with cyber-attacks, rising geopolitical tensions, and increasing regulatory scrutiny. 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 swift adaptation 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.

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 mere compliance into an engine for long-term value creation to drive brand value, 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 reduce background noise.

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

JENNIFER BISCEGLIE,
Interos Founder & CEO

Overview

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

This year, we surveyed 150 senior supply chain, procurement, and third-party risk decision makers within the financial services industry (FSI) to understand how changing industry dynamics are impacting TPRM/SCRM – bringing new insights, trends, and best practices for risk and procurement professionals.

While the overall cost of disruption has waned post-pandemic, a new wave of regulatory action – and the mandate to deliver improved customer experiences – is driving organizations to advance TPRM/SCRM maturity to achieve competitive advantage.

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

In hundreds of responses FSI leaders made clear the proliferation of digital platforms, cloud services, and remote work has expanded threat vectors, making it harder to monitor and defend against threats and while maintaining regulatory compliance. The rise of sophisticated cyber-attacks, data breaches, and ransomware demands a constant state of vigilance.

Key Findings

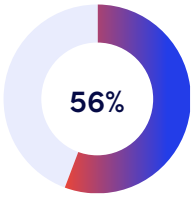
5

The average financial services organization experiences **five supply chain shocks** requiring "significant mitigating action" annually

↑ $37M

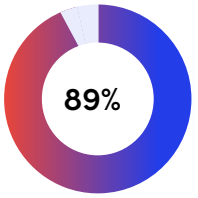
FSI organizations believe they **can recover $37M annually** by preparing better for and reacting faster to disruption

RISK ASSESSMENT



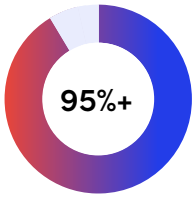
On average, FSI organizations only assess 56% of their critical suppliers for risk

RISK MANAGEMENT MATURITY



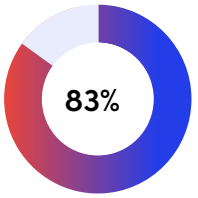
89% of FSI organizations do not consider themselves to have reached the highest level of SCRM/TPRM maturity

EVENT AWARENESS



95%+ of FSI 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



83% of financial services 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...

78 are from the **United States**

33 are from the **UK and Ireland**

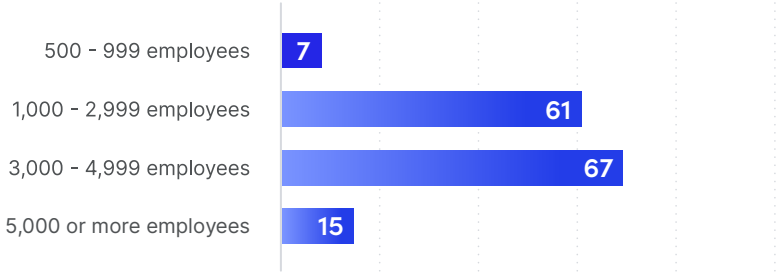
39 are from **Canada**

79 are within senior management

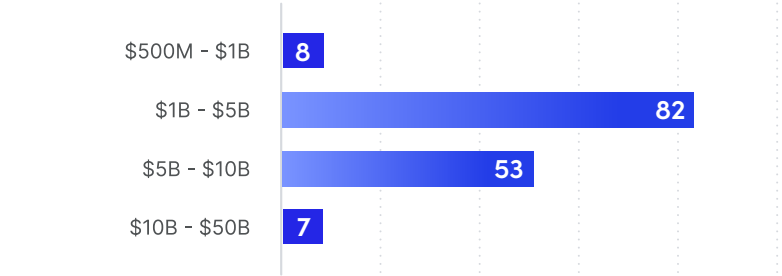
71 are C-level or board members

Demographics

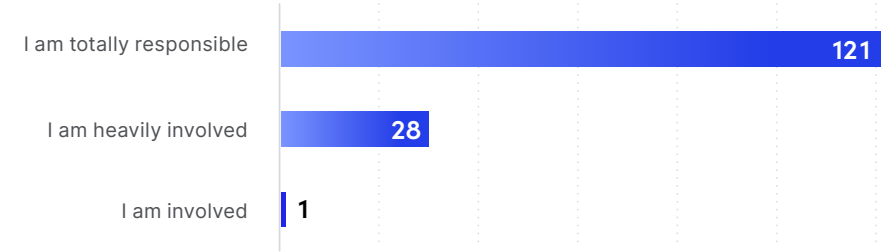
Q: How many employees does your organization have globally?



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

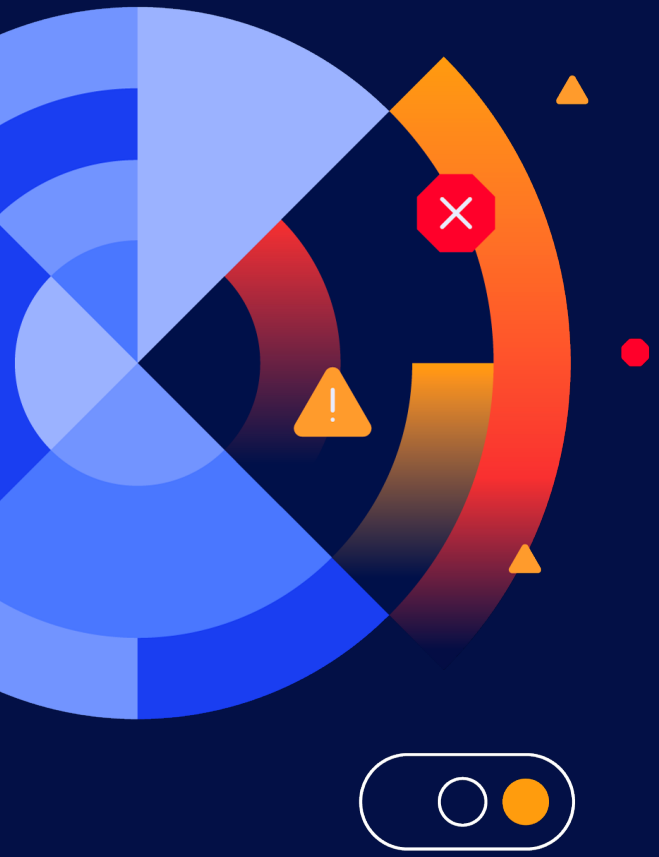


Q: What is your level of involvement when it comes to managing the global supply chain in your organization?



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 multiple other disruptive events continue to impact 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 $102M Gap

Supply chain disruptions are frequent and costly. On average, the 150 FSI organizations that participated in the study responded to five major supply chain disruptions within the past 12 months, resulting in $102M in lost revenue. These were events requiring "significant mitigating action". Mitigation included engaging backup service providers, activating cybersecurity response teams, adjusting compliance controls, or modifying client-facing services to maintain continuity.

While the overall disruption costs for FSIs dropped in comparison to our 2022 survey, the number of significant supply chains disruptions increased, from three to five annually, a 40% 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.

5 **UP 40%**
FROM 2022

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

$102M

Annual financial impact as a result of these supply chain disruptions

$23M

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

$100M

Average annual cost of disruption for FSI companies with $1B - $50B in annual revenue.

$53M

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

Costs by Vertical (in USD millions)

Survey data revealed that financial services firms suffered significantly greater losses due to supply chain disruption than aerospace & defense or government organizations. This is also true for energy and healthcare organizations. This disparity may reflect the fact FSIs rely heavily on sprawling digital networks for data processing and transaction support – making them more vulnerable to global disruption.

Conversely, 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.

Larger organizations also incurred greater costs due to disruption – though those costs did not scale 1:1 with revenue. On average, financial services companies with between $500M and $1B in annual revenue incurred costs of $53M, whereas for FSI firms with $10B - $50B in revenue the comparable figure was $100M.

> "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.

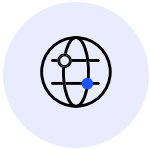
Q: What annual cost increases and/or revenue losses does your organization experience annually?

FINANCIAL

$45M

CATASTROPHIC

$43M



GEOPOLITICAL

$47M

CYBER

$45M

ESG

$45M

RESTRICTIONS

$47M

Shocks to the System: Six Major Categories of Risk

Third-party/procurement executives at financial services institutions reported annual cost increases and/or revenue losses ranging from $43M to $47M 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

Restrictions were the most expensive disruption – propelled by a surge in new controls from Western governments targeting Russian and Chinese entities. But 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.

“We’ve had to very thoroughly audit the robustness of vendors' ability to respond to challenges — where the data centres are and what their SLAs are. So, if suddenly something catastrophic were to happen, how do we ensure that we still have system access, power access?”

– Procurement Leader, U.K.

29%

of FSI organizations put cyber attacks in their top 5 risks

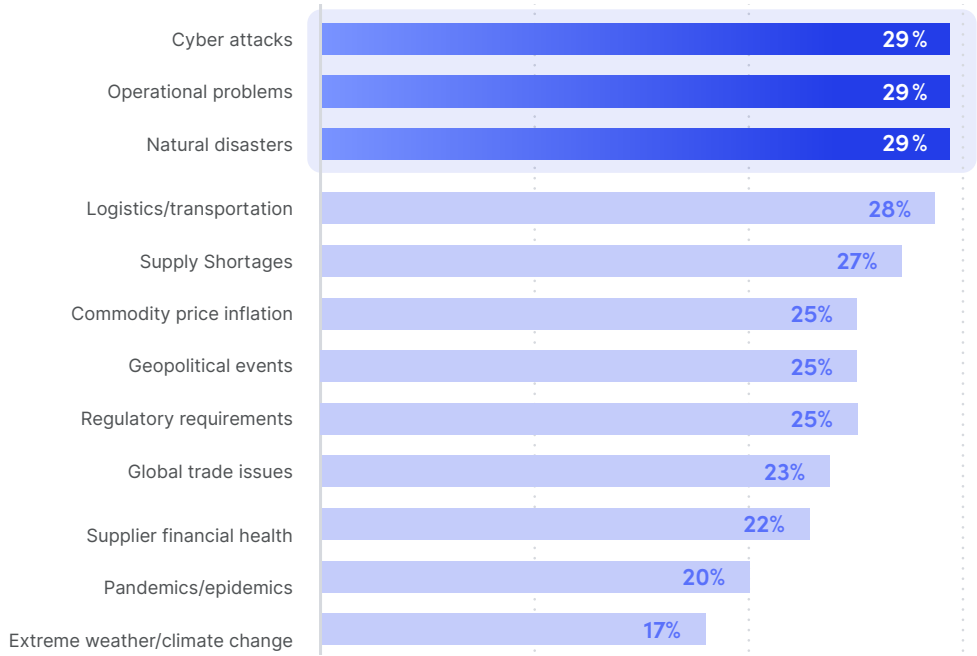
Top Crisis Triggers: Cyber-Attacks, Operational Problems

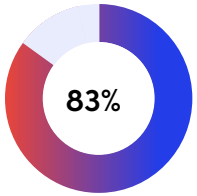
Cyber-attacks, operational problems, and natural disasters top the list of concerns for FSI procurement/third-party risk leaders by a slim margin. While FSIs are near-equally concerned about the array of threats that face, they are less concerned about physical supply chain issues, such as commodity inflation and logistics issues given the sector’s heavy reliance on digital vendors.

That reliance also explains why cyber-attacks ranked highly within FSI areas of concern though at lesser levels than risk leaders in aerospace & defense or government. This may reflect the fact that a successful cyber-attack on an A&D or government organizations can have dire implications for national security, classified data, and advanced military technologies.

FSIs are also subject to different regulatory requirements. They have historically invested heavily in cybersecurity, which may lead to a reduced perception of risk compared to A&D and government respondents.

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)





83% of FSI 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	80%
	National Defense Authorization Act (NDAA) Section 889	78%
	Interagency Guidance on Third-Party Relationships – US	76%
	Uyghur Forced Labor Prevention Act (UFLPA)	74%
	German Supply Chain Due Diligence Act	77%
	Critical Raw Materials Act – EU (proposed)	76%
	Digital Operational Resilience Act (DORA)	76%
	Corporate Sustainability Due Diligence Directive (CSDDD)	73%
	PRA/FCA Operational Resilience Regulations	74%

* Significant or moderate impact

Expanding Regulation: Legislation Will Have a Material Impact

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

Financial organizations were most concerned with the impact of changes required by Canada's Office of the Superintendent of Financial Institutions (OSFI) — the nation's federal financial institutions regulator — to Guideline B-10: Third-Party Risk Management. The guideline takes effect in 2024. It significantly broadens the scope of FSI TPRM requirements to cover all third parties a financial institution may have a relationship with – including utilities or relationships created by an institution's parent company or subsidiaries.

Three-quarters of FSI respondents say other proposed new rules in the U.K., Canada, the U.S. and the European Union – including the Digital Operational Resilience Act (DORA) – will have a moderate to significant impact on their compliance requirements.

Financial organizations shared generally greater concerns over most regulatory changes than A&D or government respondents. This is also true for healthcare and energy companies. The only area of overlap between each of these sectors is the U.S. Uyghur Forced Labor Prevention Act (UFLPA). It empowers border officials to seize shipments of products suspected of being made with forced labor in the Xinjiang region of China, and ever-tightening sourcing rules related to Chinese technology in U.S. federal government contracts (Section 889 and 5949).

83% of FSI respondents agreed they "cannot hope to comply with these laws without supporting data, analytics and risk management software." Some controls are also perceived as beneficial over the long-term; a majority of FSI procurement TPRM respondents consider it helpful in forcing supply chain and third-party risk management improvements.

83%

of FSI participants are “extremely” or “somewhat” concerned about geopolitical tensions

Top concerns from a geopolitical perspective:

1. Damage to cost efficiency from resilience-building measures
2. Increasing government focus on protectionism, national security, industrial policy and/or self sufficiency
3. Heightened threats to critical infrastructure

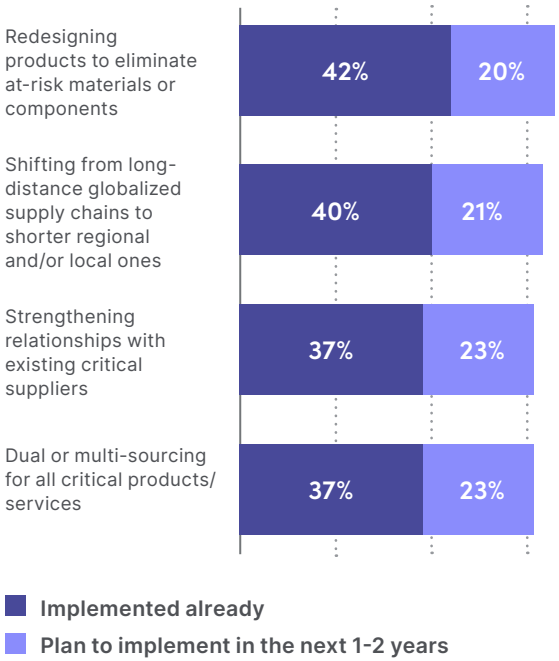
Shortages, Costs, Protectionism Are Top Geopolitical Concerns

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 agenda for all industries, FSIs included.

When asked about the potential impact of geopolitical tensions on their suppliers and supply chains over the next three years, 83% of FSI participants are “extremely” or “somewhat” concerned.

FSI procurement and TPRM leaders are most concerned about the potential for cost efficiency losses due to geopolitical strife. They are also concerned about how government industrial and national security policies are reshaping global trade in a more protectionist direction, and about increasing threats to critical infrastructure (ports, power plants, internet connectivity, etc.) from military or cyber-attacks.

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



Better Relationships, Redesigned Offerings Key to Resilience

FSIs have restructured their global supply chains and third-party networks in response to geopolitical risk events. Their top strategy was redesigning products to eliminate at-risk materials or components – a reflection of the widespread Western pullout from Russia in the wake of the invasion of Ukraine. Product redesigns are easier to make within digital supply chains. For example, phasing out vulnerable transaction processing systems or migrating a locally hosted subsystem to a cloud-based solution is substantially less daunting than building a new manufacturing facility. This is because digital networks operate without the capital-intensive costs associated with managing industrial equipment and other assets in physical supply chains – explaining why FSIs may have shown greater preference for this strategy compared to other verticals.

A clear majority of FSIs also moved to more regional or national suppliers/operations, or plan to do so in the near-term, though they were less likely than A&D or healthcare overall to pursue this. The same is true for reshoring or nearshoring key supply contracts (led by A&D and energy companies) and diversifying global footprints. This includes moving some suppliers and/or production away from China to other countries. Financial services organizations are also diversifying their vendor base through a greater use of dual- and multi-sourcing.

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

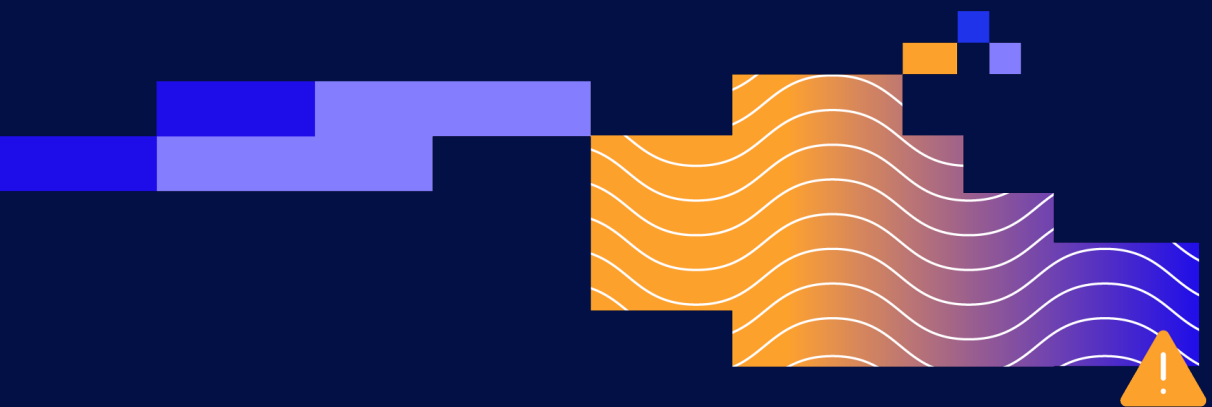
SECTION 02

The State of Supply Chain and Third-Party Risk Management

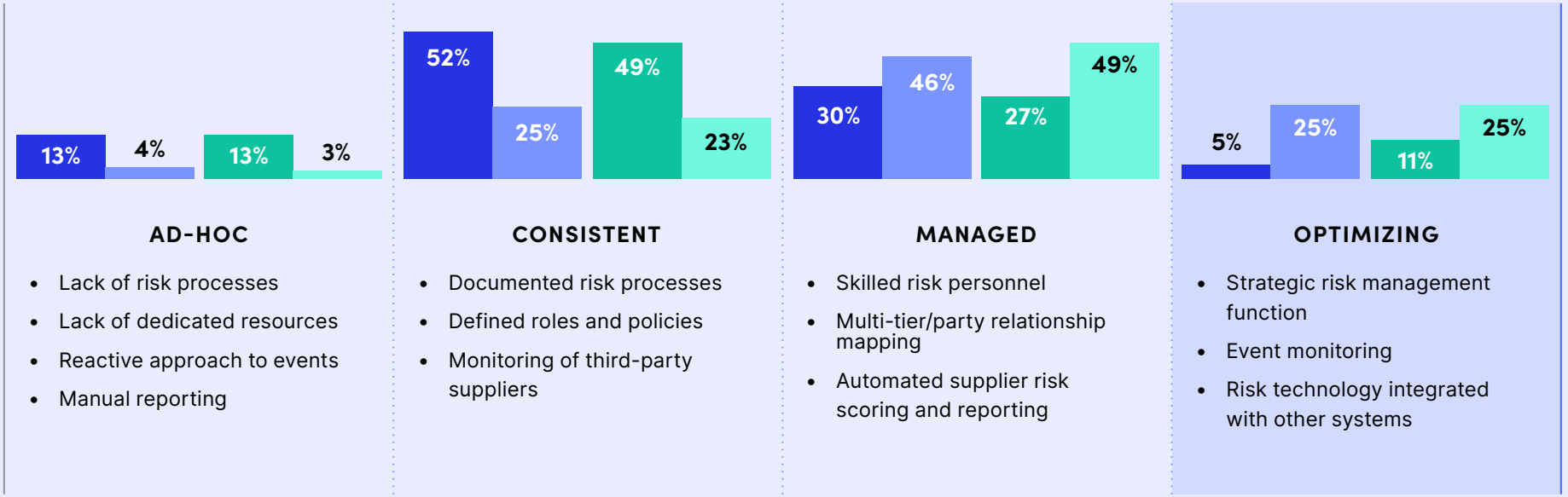
Maturity Set to Increase in Next Three Years

Despite major global supplier shocks in recent years, many financial services organizations still lack the knowledge, resources, processes and tools needed to manage and respond to third-party risks at speed and scale. An overwhelming majority (89%) of surveyed executives within financial services do not think they have reached the final stage of SCRM/TPRM maturity (see next page).

Additionally, more than half of FSI organizations (62%) self-identify at a lower level of maturity today – specifically, as “ad hoc” or “consistent” on the Interos SCRM/TPRM maturity scale – compared with less than half (38%) 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

FSI Average
- Today
- In the next 3 years

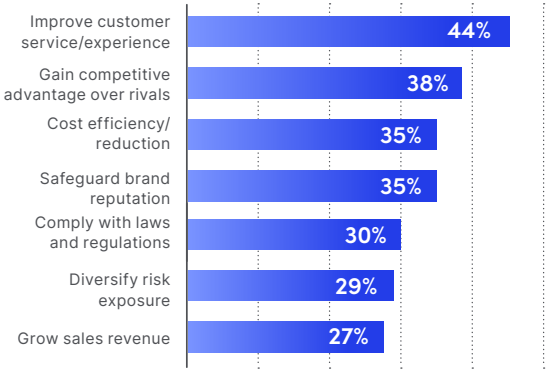
This ratio reverses when asked where they expect to be in three years, with 72% of respondents expecting to be at the mature end of the spectrum characterized by the following capabilities:

- 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 to drive execution
- Multi-tier visibility of the extended physical and digital supply base
- Automated supplier risk assessments and executive reporting
- Continuous monitoring of potentially disruptive events
- A cultural mindset shift within the organization to catalyze change

"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?



Maturity Levels Today Vary Widely Between Sectors

The overall findings mask stark differences between sectors. FSI respondents were more likely to say they had reached the final maturity level ("Optimizing") than other verticals (11% for FSI compared to A&D at 8%, healthcare/energy at 3%, and government at 1%). Looking at just the top and bottom halves of the maturity scale, less than half (39%) of FSI firms place themselves in that upper half (Managed & Optimizing), second only to A&D firms (48%). FSI organizations expect to maintain their relative position over the next three years – slightly behind A&D but ahead of our other verticals – with 74% anticipating they will reach the "Managed" or "Optimizing" stages by 2026.

For comparison, 69% of government agencies anticipate they will progress their SCRM/ TPRM capabilities to "Managed" or "Optimizing" during this period, compared with 83% of A&D firms.

Benefits of Enhanced TPRM: Customer Service, Competitive Edge, Market Leadership

The ambition to improve risk management practices is shared by all sectors. The data shows improving service delivery, with customer experience as the most common driver for improving SCRM/TPRM (44%). This is unsurprising given supply chain disruptions impact transaction speed and efficiency, platform availability, or personal information exposure, all of which erode customer trust, confidence, and market leadership. In addition to service integrity, the need to gain competitive advantage is a close second for financial services.

This differs from the survey's overall results, where improving cost efficiency was the second-most-cited driver (39%). The reduced priority may indicate that financial services institutions see themselves as having already achieved greater cost efficiency. It may also reflect the fact that within financial services, innovation, agility, and differentiation are key to success. While cost efficiency is important, focusing on robust risk management, compliance alignment, and advanced technology services can provide a more significant strategic advantage in the rapidly changing financial landscape.

Better Risk Management Has Financial Benefits

When asked to quantity the value of improved risk management, 93% of financial services participants selected an annual figure between $10M and $50M, with an average of $37M.

This includes both cost savings and increased sales (a risk improvement driver for one-third of the FSI sample) and equates to 36% of the average cost of supply chain disruptions in 2022. As with maturity, FSI firms are second only to A&D respondents ($47M on average) in optimism about the potential financial benefits of SCRM/TPRM. They are substantially more optimistic than government organizations, who were the least hopeful ($26M).

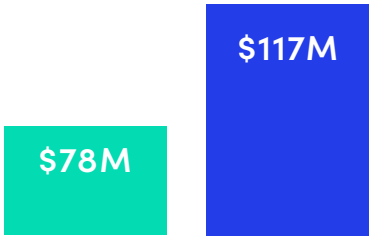
It is also worth noting that while those leaders who identify as more mature today estimate a slightly lower figure of $31M in savings (compared to $41M for their less mature peers), they also report a lower average cost of disruption ($78M versus $117M). So, financial services institutions experience 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.

FSI participants who reported a higher perceived financial benefit to reacting faster also experienced more disruptions – with organizations who thought they could save between $50M – $100M experiencing six major supply chain disruptions annually, while those who thought faster reaction would only save them between $1M - $10M experienced an average of three major annual disruptions.

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

$37M

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



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

- Mature
- Less mature

"Our supply chain has to be seen as providing us with a competitive advantage. We have to provide end-to-end planning, visibility and collaboration."

– Procurement Leader, U.S.

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

1	Lack of reliable data to inform goal-setting and progress tracking	42%
2	Lack of financial resources/ investment budgets	41%
3	Lack of visibility into sub-tiers of extended supply chain	39%

ESG is Core to Safeguarding Brand Reputation

More than one-third (35%) of our FSI 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. Almost half (47%) say they are stepping up ESG supply chain activities and investments – a greater percentage than any other industry surveyed (40% for healthcare, 36% for A&D, 34% for energy, and only 18% for government).

A substantial percentage, just under half (41%) of FSI TPRM/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.

Respondents say they've made the greatest strides in ESG third-party risk management across the following areas over the past three years:

- Environmental pollution
- Renewable energy
- Working conditions
- Forced labor

Core ESG Challenges: Usable Data, Sub-Tier Visibility

Despite the importance of ESG objectives to FSI organizations and supply chain/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, insufficient financial resources/budget, and poor sub-tier visibility were also cited as barriers to ESG progress. All three are critical in the ESG domain, where violations of environmental and social standards can often occur further upstream in supply chain and third-party networks where organizations have 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**	**83%**
New regulatory requirements help us to improve collaboration and information sharing with our **direct (tier-1 or third-party) suppliers**	**79%**
New regulatory requirements force us to improve our awareness of critical **indirect (e.g., tier-2/3 or fourth/fifth party) suppliers**	**79%**

Regulations Promote Better Risk Management

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

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

A similar percentage (82%) say that new laws compel them to invest in risk processes, people and technology. The same percentage agree this is critical to ensure compliance. Seven out of 10 go further than basic compliance, welcoming stricter laws on the grounds they are an opportunity to gain competitive advantage against rivals; this is the top driver for FSIs to invest in TPRM/SCRM.

Regulations Promote Collaboration and Awareness

Similar numbers of FSI TPRM and procurement executives believe 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 79% of FSI survey participants. This is an essential foundation for maturing SCRM/TPRM capabilities and driving greater operational resilience.

SECTION 03

Developing Operational Resilience

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

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

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

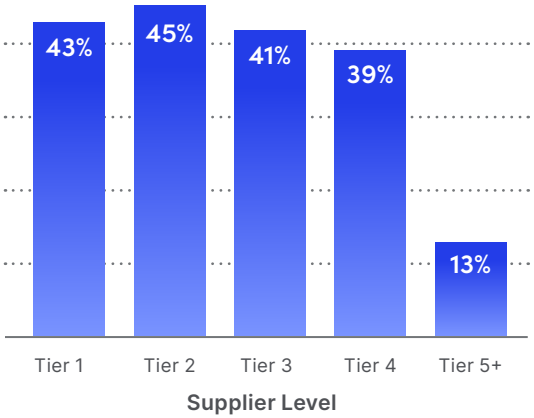
3. **Monitor** events across their global networks in real time or near real time, so they can pre-empt disruption before it strikes and/or react quickly when required

Mapping, modeling and monitoring are important parts of an ecosystem-based approach to supply chain and third-party risk management. It's designed to identify issues and potential sources of disruption earlier and faster.

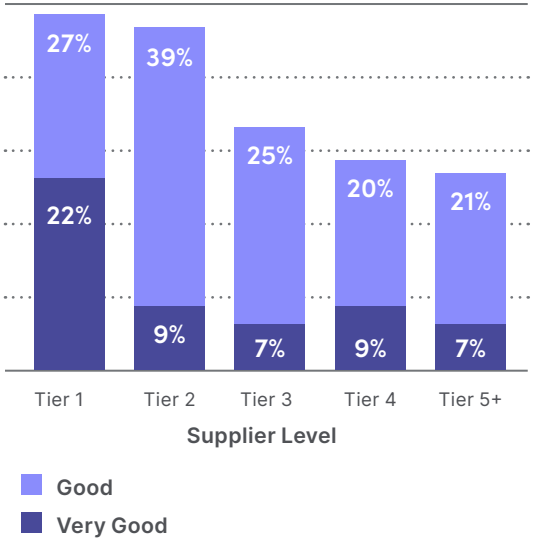
How Interos Defines Operational Resilience

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 strategic decisions about where to invest in contingency options.

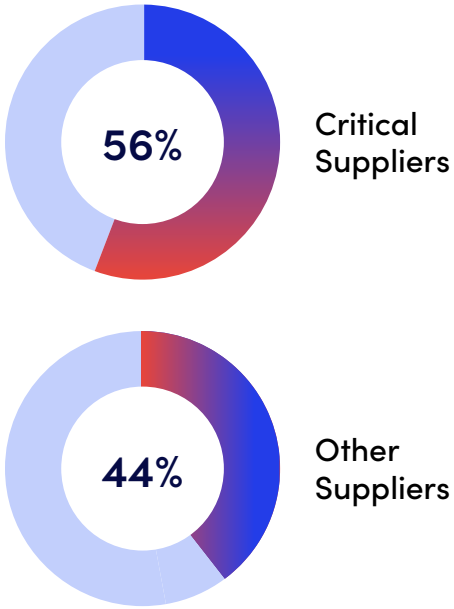
Disruptive third-party events – whether a supplier bankruptcy, a factory fire, a cyber-attack, or another incident – often originate among sub-tier or nth-party suppliers. Our survey data shows that in the past 12 months tier-2 or fourth-party suppliers were the most common source of disruption for financial services organizations, followed by those at tier-1/third parties. However, they were only a few percentage points ahead of tier-3/fifth parties and tier-4/sixth parties. Similar responses indicate that effective TPRM/SCRM programs must monitor relationships beyond the third-party.

And financial services organizations have significant work to do here (as do the other industries surveyed). When asked about visibility levels at tier 2, less than half (48%) of FSI 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 tiers 3, 4 and 5+, one-third or less believed they had this degree of information.

FSI respondents estimated similar levels of visibility to those in the healthcare, government, and energy industries across all tiers/parties. They fell short only to A&D firms who were 16-19% more likely to say they had good/very good visibility across tiers 1, 2 and 3 than the average for all organizations. But A&D fell back in line when it came to tiers 4 and 5+. Clearly there is room for widespread improvement.

> "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 FSIs also need to know how risky individual third parties are, and across what specific risk dimensions. The risk assessment component of modeling addresses this, providing information that procurement and risk managers use for more focused decision making and prioritization.

Survey participants were asked to distinguish between "critical" suppliers/third-parties – those essential to business units, provide critical products and services, have good strategic fit with their customer, and so on – and "other" suppliers. Within FSIs, only 56% of critical suppliers and 44% of other suppliers are subjected to a risk assessment during the sourcing and/or third-party/supplier management process, on average.

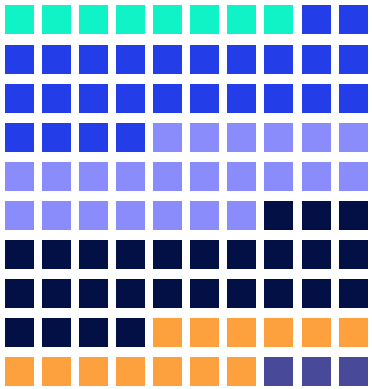
This was consistent across industries, except A&D, which boasted somewhat better coverage, as did larger or more mature organizations. Even here the figures are relatively low compared with where they should be for security, compliance and operational resilience purposes.

> "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

"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 - **8%**
- Weekly - **26%**
- Quarterly - **23%**
- Every six months - **27%**
- Annually - **13%**
- Ad Hoc - **3%**
- Never - **0%**

3. Risk Monitoring Needs to Be Continuous

A necessary part of effective supply chain and third-party is robust due diligence and certification checks during the supplier selection process, followed by key supplier auditing to validate policies and practices (for example, around ESG) during the contracting process. But in a dynamic, fast-changing risk landscape, these periodic interventions are insufficient to anticipate disruptive events. Organizations need continuous monitoring across their extended supply chains to achieve an the most accurate assessment of vendor risk.

Just 8% of FSI procurement/TPRM leaders say they monitor their most critical suppliers daily, with 26% indicating weekly (more mature organizations are slightly higher on both frequencies). 50% conduct risk monitoring on a quarterly or biannual basis. For other suppliers, the frequencies are lower still, with 26% saying they only do this once a year. On average, FSI organizations assess critical suppliers every 17 weeks – more frequently than the cross-industry average of 20 and more frequently than any other industry surveyed. However, FSI organizations assess "other" suppliers every 26 weeks (less frequently than the cross-industry average of 20). This leaves organizations vulnerable to unexpected and unpredictable risk events.

Notably, FSI organizations that report positive economic expectations for 2023 assessed critical suppliers much more frequently (every 16 weeks) compared to those with negative expectations for the year (every 33 weeks).

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	4%
...disrupted by a geopolitical issue	3%
...experiences an operational disruption	5%
...disrupted by extreme weather/natural catastrophe	2%
...becomes the subject of a restriction/ sanction	2%

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 any negative impacts. The first few days after an incident are a critical window for situation assessment and action planning. This includes implementing alternative digital transaction channels, engaging backup service providers, activating cybersecurity response measures, adjusting compliance controls, and modifying client-facing services to maintain continuity.

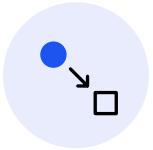
Less than 5% of FSI procurement and third-party risk leaders say they are aware of various risk events within 48 hours of occurrence across every tier of their supply chain. Around half of our sample have either no visibility of a third-party risk event – cyber-attack, ESG violation, insolvency, etc., within 48 hours or only have visibility at the tier-1 level – so significant improvements are needed.

A further one-third of our FSI 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 15% more likely to say that they would have 48-hour notification of cyber or geopolitical events at the lower tiers of their supply chains than those that are less mature today.

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

57%
People



63%
Processes

55%
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 and third-party risk leaders within financial services are generally optimistic about the remainder of 2023, with 93% positive about their organizations' financial outlook (in contrast with government, where 49% are negative). This optimism translates into expectations about the resources they anticipate having to manage risk. The majority expect to grow their investments in people, process and technology this year, while between 16% and 33% say spending will be flat in each of the three areas.

More mature financial services organizations are more likely to say they are significantly increasing their investments in technology, 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

Enrich or speed up due diligence during supplier selection and onboarding

Data/analytical support for risk mitigation

Multi-tier supplier relationship visibility

"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 Identification, Decision Support

FSIs consider the two greatest operational benefits of SCRM and TPRM technology solutions to be enriching and/or speeding up due diligence during supplier selection and visibility of multi-tier supplier/third-party relationships and dependencies. But just eight percentage points separate these benefits from others that respondents ranked among their top three – namely, identifying risky suppliers across multiple factors, data/analytical support for risk mitigation, and multi-tier supplier relationship visibility.

From an industry vantage point, FSI leaders were less likely than other industries to consider the ability to identify high-risk suppliers across multiple factors the key benefit of technology. This could indicate that financial services firms have greater preference for their more-established methods for risk assessment or that they prioritize other aspects of supplier relationships, such as alignment with the company's strategic goals, and integration with existing systems.

They were also slightly more likely to value enriching and/or speeding-up due diligence during supplier selection than other sectors. This likely reflects a concern with ensuring that suppliers meet the specific regulatory standards and align with the rapid pace of the financial sector.

FSI organizations with more mature TPRM/SCRM programs valued some technology benefits more than their less-mature peers. More mature organizations were much more likely (19% - 23%) to see value in the following benefits than less mature ones:

- The ability to identify high risk suppliers across multiple factors
- Rapid notification of risk events and potential disruptions

SECTION 04

Recommendations for FSI Risk Leaders

- **Invest in continuous, multi-tier supply chain risk visibility.** Only 8% of financial services companies continuously monitor their suppliers, and most lack sufficient visibility of all tiers within their supply chains. Without this level of insight, companies are relying on lagging risk indicators that leave them vulnerable to pending disruption and falling behind competitors who are seizing the advantage comprehensive and continuous visibility provides.
- **Ensure risk insights are meaningful.** Ensuring visibility across multiple tiers/parties is only a partial step. Successful risk programs need to ensure the insights they have into those tiers achieve the appropriate level of granularity – information sufficient to identify and act on the vulnerability or disruption – and are being delivered to the right decisions makers in time to take effective mitigation actions.
- **Apply and track progress against a maturity model.** More mature organizations have lower costs associated with disruption – and 89% of FSIs think they need to improve risk management capabilities. To start realizing these benefits, organizations need to begin investing in documented processes, strategic risk functions, skilled personnel, and risk technologies that 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 financial services organizations do not know about a supplier disruption in the first 48 hours, leaving them flat footed in a stakeholder environment that demands a rigorous, timely, and ethical corporate response. By investing in resilience, organizations can increase the scope of disaster recovery activities to include their third parties – bridging the gap between third-party risk 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.** Third-party/supplier risk management accountability may rest most often with the procurement function (and does for 34% of our FSI 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 survey participants. Collaboration requires identifying and mapping who those critical partners are, then sharing information and in some cases, making shared investments to mitigate the most critical risks. All of this is more difficult, if not impossible, to achieve without a corresponding level of open communication and trust between buyer and supplier.
- **Harness technology for efficiency and actionable intelligence.** In larger organizations, today's vast and interdependent SCRM and TRPM are too complex to manage via spreadsheets. Advanced software and data analytical capabilities are essential for identifying, assessing, mitigating and monitoring supply chain risks on a continuous basis. It is not surprising that a majority of respondents plan to increase their technology investments this year. Effective supplier risk specialists spend the bulk of their time preparing their organizations for and responding to impactful events, not gathering data.

Closing Thoughts: Making Order from Chaos

The increasingly complex and volatile global landscape makes it imperative for financial services organizations to bolster their supply chain and third-party risk management strategies. FSIs believe that a wide swath of actions – from enhancing multi-tier visibility and data granularity to fostering both internal and external collaborations – are essential. Technology is seen as a key enabler for efficiency and actionable intelligence. As the sector evolves, organizations that take a comprehensive, agile, and technologically advanced approach to managing risks will not only mitigate disruptions but also gain a competitive advantage in a marketplace that demands resilience.

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

091223