The 2026 Supply Chain Risk Report

Sphera survey data (2025)

REPORT 2 OF 2

sphera

What's Inside

Executive Summary	**3**
The Confidence Gap (the paradox lives here)	**5**
Governance: Scrutiny and Defensibility Requirements	**8**
Outcomes: Disruptions and Loss Remain Widespread, While Key Risks Rise	**10**
Where Leaders Think Risk Comes From vs Where It's Materialising	**12**
Why the Resilience Playbook Plateaued	**14**
The Bottlenecks: *N*-Tier Visibility, Supplier Engagement, Data Integrity, and ROI	**16**
Operating Tempo: Desired Speed vs Actual Cycle Times	**20**
AI: Adoption Is High, Impact Is Capped by Foundations	**22**
2026 Implications: 7 Concrete Shifts	**24**

Executive Summary.

The 2025 survey data provides a perception-based view of how organisations assess their supply chain risk readiness heading into 2026. The analysis draws on four Censuswide surveys commissioned by Sphera quarterly throughout 2025, capturing responses from 800 Chief Procurement Officers and Chief Supply Chain Officers across the United States, United Kingdom, Germany and Canada. When read alongside Sphera's incident monitoring data, a clear pattern emerges: leaders express very high confidence in their capabilities, yet the outcomes and constraints they report, point to underlying structural fragility that continues to drive disruption and loss.

Governance pressure is now continuous. Supplier and supply chain risk decisions are challenged frequently by boards, CFOs and senior executives (48.5% weekly/monthly; 46.5% quarterly). This is not episodic oversight. It reflects an operating environment where supply chain risk decisions are treated as strategic and financially material, and where teams are expected to justify recommendations with defensible evidence.

Confidence, however, remains near-universal at the headline level. Respondents report extremely high confidence in the completeness and currency of supplier risk data (98% confident; 66% very confident), in their ability to detect supplier financial distress before escalation (100%), and in the accuracy and completeness of supplier data used for ESG and compliance reporting (99%). On the surface, these figures imply mature risk intelligence, deep visibility and strong early-warning capability.

4

Surveys
Censuswide surveys by Sphera quarterly through 2025

800

Participants
Chief Procurement Officers and Chief Supply Chain Officers

4

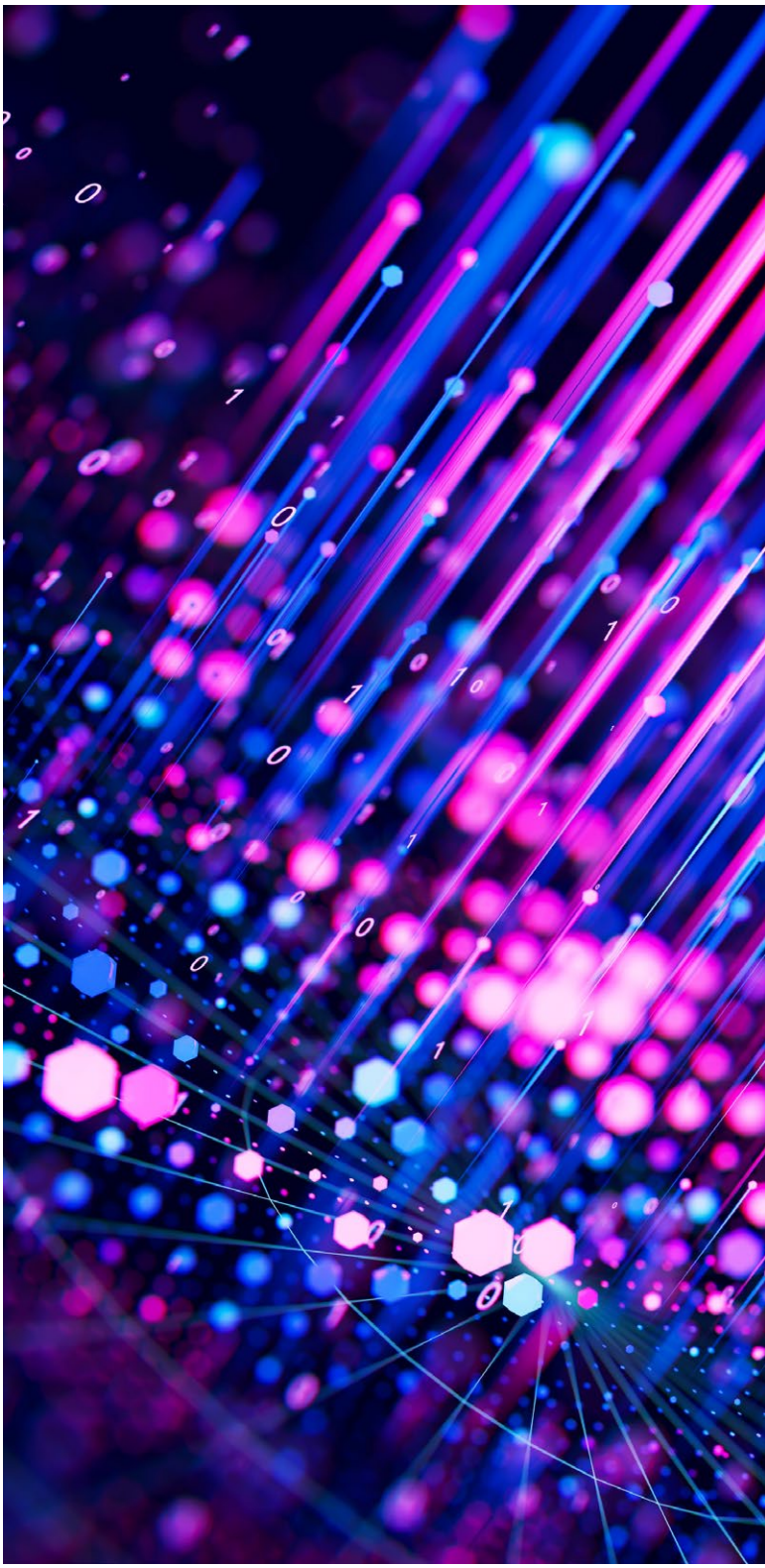
Countries
United States, United Kingdom, Germany and Canada

But outcomes and detailed survey responses do not fully support that perception. Most organisations continue to experience financially material disruption impacts: 73% report financial or operational losses due to supply chain disruptions in the past 12 months, and in the financial-health/commodities survey the mean number of material disruptions is 3.48. When the survey moves from broad confidence statements to practical questions about how visibility is achieved, barriers appear repeatedly: lack of supplier cooperation and data sharing, poor data quality and completeness beyond Tier 1, fragmented tools, limited internal capacity, and the need to justify ROI for further investment.

Incident data reinforces that the risk environment is not stabilising evenly. Viability remains the largest category by volume and continues to rise; quality is the fastest-growing; ESG/compliance pressure is increasing with concentrated late-year spikes; delivery improves in aggregate but remains operationally volatile. The overall picture is not a system with uniformly declining risk, but one where stress is clustering and shifting.

Most organisations also report that they have already executed the classic resilience playbook: diversification, near-shoring, buffer increases, expanded monitoring tools and AI adoption. That suggests a plateau. The remaining constraints are structural rather than tactical: verifiable N-tier visibility, supplier engagement at scale, data integrity, and CFO-ready value justification.

The defining 2026 story is therefore a gap between perceived maturity and measured exposure. Leaders feel confident and are under constant scrutiny, yet disruption remains common and key risk categories continue to rise. Closing that gap will require less emphasis on “more tools” and more emphasis on foundational capability: auditable upstream visibility, validated data, integrated intelligence, faster decision cycles, and targeted interventions where risk concentrates.

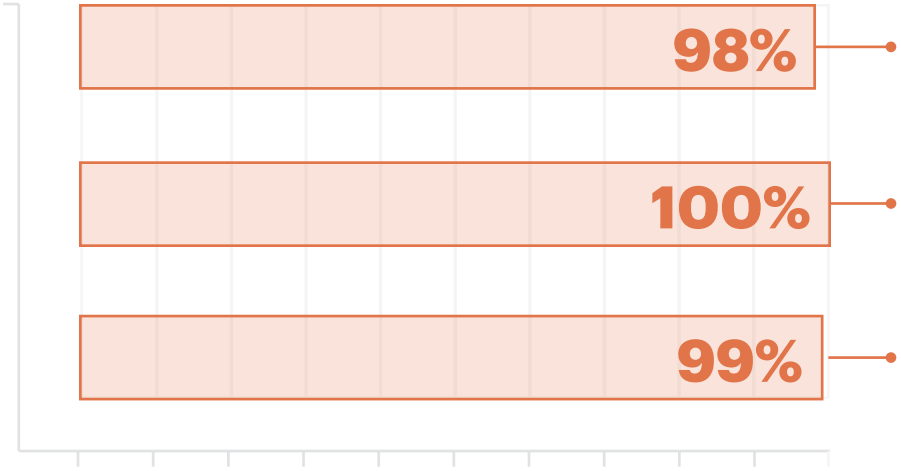


The Confidence Gap (the paradox lives here)

Across all surveys, confidence is strongest when questions are framed broadly and weakest when questions become operational and specific. This creates a consistent confidence gap: leaders express high certainty about the quality of their supplier risk intelligence, yet simultaneously acknowledge constraints that directly undermine that certainty—particularly beyond Tier 1.

Headline confidence is near-universal.

While respondents report near-universal confidence at a high-level, the data reveals conflicting realities in operational execution.



Respondents report:

- confidence that procurement/supply chain decisions are **based on complete, up-to-date supplier data** (66% very confident).
- confidence in the ability to **detect supplier financial distress** before it escalates (50% fully confident).
- confidence in the **accuracy and completeness of supplier data** used for ESG and compliance reporting.

But the survey also surfaces structural weaknesses that conflict with that confidence.

Respondents cite:

44.5% **lack of accurate and up-to-date supply chain data** as a barrier to achieving visibility and effective contingency planning.

32.4% **poor data quality** and/or **completeness** as a major challenge in obtaining accurate Tier-2+ supplier data.

34.8% **lack of supplier cooperation** or **data sharing** as a major barrier to meaningful upstream visibility.

Perceived depth of visibility conflicts with prioritisation and constraints.

On perception-based questions, organisations report strong upstream visibility:

52% claim **extensive visibility** beyond Tier 3 suppliers.

43.6% report **moderate visibility** beyond Tier 2 and some Tier 3.

Yet the same dataset contains clear signals that visibility is incomplete or inconsistent:

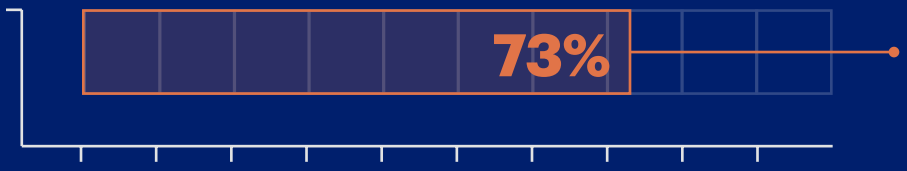
39% acknowledge **limited visibility** beyond Tier 1.

40.8% prioritise **expanding supply chain mapping** beyond Tier 1 within the next 12–18 months.

This conflict suggests that "visibility" is often being defined loosely (partial Tier 2 awareness, limited to critical suppliers or crisis response) rather than as continuous, validated and usable *N*-tier intelligence.

Disruption outcomes challenge the implied effectiveness of early warning.

Despite reported confidence in detection and data completeness:



report **financial or operational losses** due to disruptions in the past 12 months.

In the financial-health/ commodities survey, the mean number of material disruptions reported is 3.48.

Only 5.5% report zero disruptions.

If early-warning capability were consistently strong and decision-ready, these outcomes would be expected to be materially lower.

The confidence gap is not complacency; it is misalignment between outputs and foundations.

The survey results point to confidence being expressed at the outcome layer—dashboards, summaries, and reporting artefacts—while the underlying foundations remain variable: supplier cooperation, upstream completeness, validation, timeliness and integration across systems.

What this gap means for 2026.

Under constant governance challenge, confidence must be supported by evidence. The core risk entering 2026 is not that leaders lack intent or tools, but that perceived readiness is not consistently matched by auditable data quality, verifiable *N*-tier visibility and decision-speed capability. This mismatch drives scrutiny and contributes to recurring disruption-related loss.

Governance: Scrutiny and Defensibility Requirements

The survey data shows that supply chain and supplier risk decisions are now subject to routine governance challenge, with boards and CFOs engaging frequently and directly. The implication is not simply higher oversight—it is a shift in what "good" risk management looks like: decisions must be defensible, traceable and supported by evidence that withstands executive scrutiny.

Scrutiny is embedded and frequent.

48.5%

Report supplier or supply chain risk decisions are challenged **weekly or monthly**.

46.5%

Report challenges **quarterly**.

5%

Only 5% report challenges as **rare**.

0%

0% say "**never**."

This frequency indicates that risk governance is now part of the operating cadence. Risk decisions are being contested as strategic and financially material, not treated as operational housekeeping.

Confidence is high, but governance challenge suggests a demand for proof.

Near-universal confidence in data completeness and early warning (98–100%) coexists with near-universal executive challenge. This combination implies that governance is not satisfied with high-level assurance; it requires decision narratives that can be audited and defended.

Defensibility is becoming the key governance currency.

As challenge frequency increases, organisations require:

A clear chain from signal → assessment → decision → action.

Evidence that is timely, verifiable and consistent across functions.

Documentation that supports repeatability and reduces reliance on individual judgement.

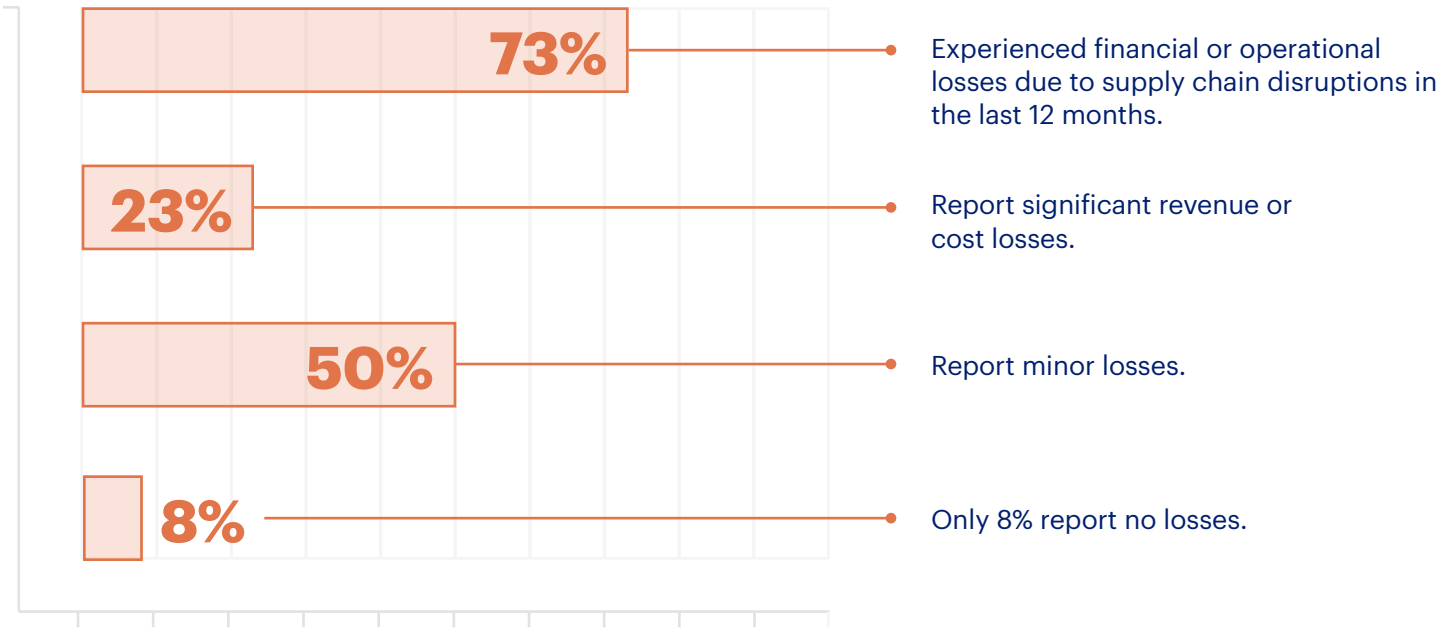
The governance risk entering 2026.

If decisions are scrutinised weekly or monthly, governance cannot be supported by ad-hoc analysis, fragmented tools or manual reconstructions of supplier risk exposure. Boards and CFOs will increasingly test not just the conclusion, but the integrity of the data foundation and the speed at which organisations can update their assessments when conditions change.

Outcomes: Disruptions and Loss Remain Widespread, While Key Risks Rise

The survey outcomes do not support a narrative of disruption becoming exceptional. Loss and operational impact remain common, and incident trends indicate that several risk categories are structurally rising—especially those that are harder to mitigate through classic resilience tactics alone.

Disruption-related impact is the operating baseline.



In the financial-health/commodities survey, the mean number of material disruptions is **3.48**, and only **5.5%** report zero disruptions.

These figures establish that for most organisations face at least one meaningful disruption per quarter, even while reporting strong early-warning confidence.

Incident data indicates structural pressure and clustering.

The incident trends show uneven improvement and increasing pressure in specific categories:

Viability

- Highest incident volume in every quarter, every year.
- Rising year-on-year from an already elevated base, with a notable Q3 spike in 2025.

Interpretation: viability is the structural anchor risk. Financial and structural fragility is persistent, not episodic.

Delivery

- Multi-year decline and stabilisation, but with early-year volatility.

Interpretation: delivery has improved in aggregate but remains a management problem, not a solved one.

Image & Compliance (ESG)

- Modest change through 2024 followed by stronger growth in 2025, with a pronounced Q3 increase.

Interpretation: ESG/compliance risk is rising and clustering, likely tied to reporting cycles, regulatory milestones and stakeholder scrutiny.

Quality & Performance

- Smallest absolute category but fastest-growing, with sharp increases across all quarters of 2025.

Interpretation: quality is becoming a faster-moving early indicator of systemic supplier stress, and even low incident volumes can translate into outsized financial and reputational impact.

What the outcomes imply for 2026.

The system is under more stress than headline confidence suggests. Loss is not an outlier; it is normalised. Meanwhile, the rising categories—viability, ESG/compliance and quality—require deeper upstream intelligence, better data integrity and active supplier engagement to mitigate.

Where Leaders Think Risk Comes From vs Where It's Materialising

The survey reveals a leadership mental model dominated by external shocks, while incident patterns indicate that several of the most material risks are emerging inside supplier ecosystems as structural stress signals.

Leaders prioritise macro forces as the most disruptive risks.

35.5%

geopolitical tensions

24.5%

macroeconomic instability

15.5%

regulatory compliance

15.5%

supplier financial health

8.5%

environmental or climate-related disruptions

This framing reflects a world shaped by trade restrictions, export controls, sanctions exposure, tariffs, inflation/interest-rate volatility and regulatory expansion.

But incident patterns emphasise supplier-level stress signals.

In contrast, incident data points to risks originating inside the supplier network:

- **Viability is consistently the largest and rising.**
- **Quality is accelerating fastest.**
- **ESG/compliance is increasing and clustering.**
- **Delivery is improving but still volatile.**

This indicates that risk is not only arriving as external shocks; a significant portion of risk is manifesting as internal supplier-network fragility that can often be detected and influenced earlier—if data and engagement foundations are strong.

Why the mismatch matters.

Budget and attention may skew toward **macro monitoring** and **scenario planning** while underinvesting in **upstream visibility**, **supplier engagement** and **data integrity**.

Boards may interpret supplier disruptions as **unpredictable external events**, when some categories show **emerging early signals**.

Mitigation may over-focus on **reconfiguration** (near-shoring, diversification) rather than **stabilisation** of high-risk suppliers and categories.

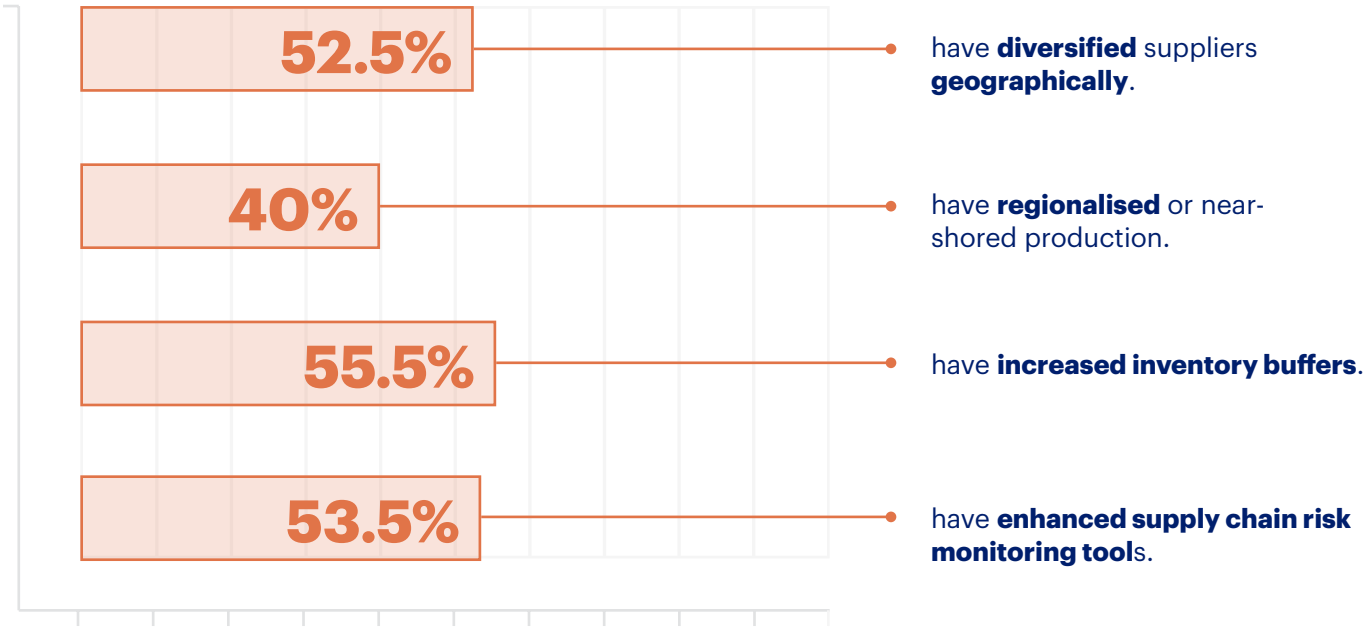
The 2026 implication.

External shocks will remain real, but the most actionable leverage often sits inside the supplier ecosystem. Organisations that align their mental model with where risk is actually materialising will allocate investment more effectively and build more defensible governance narratives.

Why the Resilience Playbook Plateaued

The survey demonstrates that organisations are not at the beginning of resilience transformation. Many have already implemented the standard levers associated with the post-2020 resilience cycle. Yet disruptions and losses persist, which implies diminishing returns from the classic playbook.

High adoption of traditional mitigation actions.



Financial hedging sits in the **low-to-mid 40% range**.

When including planned actions, adoption rises to **80–90%** for almost every measure.

Why disruption persists despite these moves.

1

These measures absorb shocks but do not fix structural causes.
They reduce exposure to immediate disruption effects, but they do not resolve supplier financial fragility, poor data integrity, ESG non-compliance or quality deterioration.

2

Diversification often occurs within correlated risk clusters.
Geopolitical and macro impacts spread quickly across regions and categories; diversification across similar profiles limits benefit.

3

Monitoring tools do not overcome weak data foundations.
Supplier cooperation gaps, incomplete upstream data and fragmented systems cap the value of additional alerts and dashboards.

4

Supplier-network stress is rising faster than mitigation capacity.
Incident patterns in viability, quality and ESG indicate underlying stress that requires targeted interventions, not only portfolio-level reconfiguration.

The plateau entering 2026.

The next stage of resilience will not be won by repeating the same levers at higher volume. It will be won by strengthening foundations that make those levers effective: verifiable visibility, validated data, and supplier engagement at scale.

The Bottlenecks: *N*-Tier Visibility, Supplier Engagement, Data Integrity, and ROI

The survey data repeatedly points to the same structural bottlenecks. These are not tactical issues; they are the limiting constraints that prevent confidence, tools and monitoring from translating into reduced disruption and loss.

1 *N*-tier visibility: claimed maturity vs demonstrated capability

High perceived visibility.

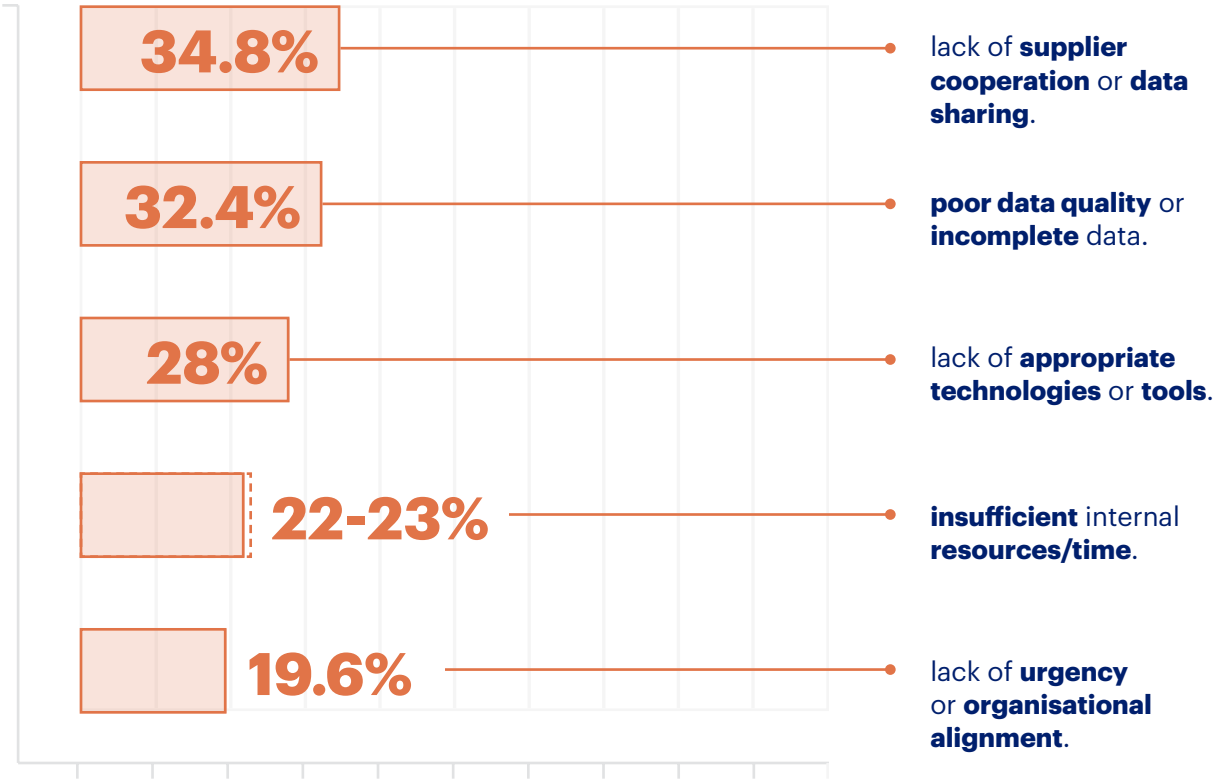
52% claim **extensive** visibility beyond Tier 3.

43.6% report **moderate** visibility beyond Tier 2 and some Tier 3.

0.4% report **no** visibility beyond Tier 1.

87.6% use or would use **technology to track *N*-tier suppliers**.

But practical barriers are widespread.



Single greatest barriers to comprehensive mapping.

23.6%
high cost of mapping/ transparency initiatives

22.4%
complexity

18%
limited access to appropriate technologies

14.4%
lack of supplier cooperation/ trust

14%
insufficient internal expertise/ capacity

Interpretation: visibility is often partial, inferred, supplier-reported, or limited to select suppliers/categories rather than continuous, validated and scalable.

2 Supplier engagement: the central constraint

When asked about barriers to resilience and visibility, supplier engagement appears consistently as the biggest blocker:

55%

cite challenges with supplier engagement and collaboration.

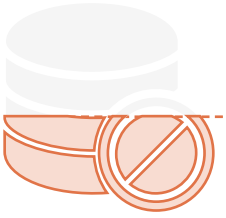
Beyond Tier 1, **lack of supplier cooperation/ data sharing** is repeatedly identified as a **major** obstacle.

Interpretation: without supplier participation, upstream visibility cannot be validated, and risk signals surface late—often only after downstream impacts appear.

3 Data integrity: confidence in outputs, fragility in inputs

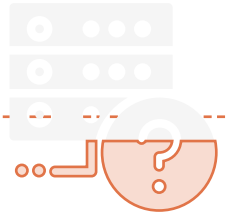
Even with 98–99% confidence in data completeness and ESG reporting data, the survey highlights:

44.5%



cite lack of accurate/ up-to-date data as a barrier.

32.4%



cite poor data quality/completeness for Tier-2+.

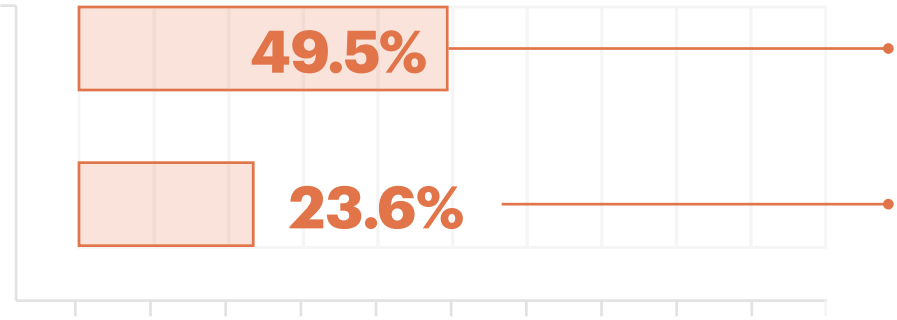
35%

report fragmented risk monitoring tools.

Interpretation: data integrity problems are not abstract—they are operational blockers that undermine governance defensibility and slow decision cycles.

4 ROI and budget: the hard ceiling on further investment

Respondents report that financial constraints are among the dominant barriers:



cite **budget availability** or ROI justification as a **barrier to resilience**.

cite **high cost** as the greatest **barrier to *N*-tier mapping**.

Interpretation: investment decisions are increasingly governed by CFO scrutiny. The requirement is shifting from "we need more tools" to "show measurable impact on disruption frequency, cost, and strategic resilience."

Operating Tempo: Desired Speed vs Actual Cycle Times

Speed is one of the clearest indicators that many organisations remain reactive rather than proactively decision-ready. The survey shows that leaders want fast insight and believe tools can deliver it, but the actual pre-decision workflows remain slow.

Pre-decision risk review timelines remain long.

65%
take more than a day and up to a week to complete pre-decision risk assessments.

30.5%
take more than a week and up to a month.

4.5%
Only 4.5% complete a risk review in less than a day.

Interpretation: sourcing and supplier decisions are still constrained by manual data gathering, fragmented tools, alignment cycles and approval bottlenecks.

Crisis response is faster than pre-decision readiness.

40%	detect, assess and respond within **3–12 hours** once a disruption occurs.
21%	respond within **13–23 hours**.
17%	respond within **1–2 days**.
~19	Average response time is **~19 hours**.

Interpretation: organisations can move fast when forced into crisis mode, but they do not operate at that speed as a default.

Desired tempo reflects the external risk environment.

< a day

27%

want insight on major external shocks in **less than a day**.

within a day to a week

60.5%

want it within **a day to a week**.

The structural takeaway.

Speed of intelligence does not equal speed of decision-making. Without validated upstream data, integrated tooling and compressed governance cycles, "real-time insight" cannot produce real-time decisions. This is one reason disruption impact remains high even as tool adoption expands.

AI: Adoption Is High, Impact Is Capped by Foundations

AI is now mainstream technology in supplier and risk management. Respondents credit AI technology with faster decisions, improved triage and stronger executive defensibility. But the broader survey findings show AI is being layered onto data and engagement foundations that are still inconsistent.

AI adoption is widespread.

94.5%

report **AI is integrated** into supplier or risk management.

50.5%

report **full integration** (automated detection and reporting).

44%

report **partial integration** (summaries, alerts, triage).

4.5%

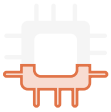
are in **pilot**.

1%

report **no AI use**.

Interpretation: AI is no longer a novelty; it is a baseline expectation.

AI is the dominant early-warning mechanism for financial distress.



40%

rely on **AI-generated risk alerts/automated monitoring**.

25.5%

rely on **credit ratings/ financial ratios**.

20%

rely on **payment delays/credit limit breaches**.

This indicates strong reliance on automated signal detection.

Perceived benefits are strong, but outcomes remain volatile.

Respondents credit AI-generated summaries with:

31%

faster operational decisions

29%

faster strategic decisions

23.5%

speed + accuracy

15%

improved defensibility with boards/CFOs

Yet disruption loss remains widespread and incident categories (especially quality and viability) continue to rise.

Why impact is capped: AI depends on foundations that remain weak.

The same survey data highlights:

- **supplier cooperation gaps**
- **poor data quality**
- **fragmented tools**
- **limited resources**
- **difficulties validating upstream information**

Interpretation: AI can accelerate detection and summarisation, but it cannot compensate for missing, delayed or unverified upstream data. Where foundations are weak, AI tends to improve speed and communication more than it reduces underlying exposure.

2026 Implications: 7 Concrete Shifts

The combined survey and incident signals point to a concrete set of capability shifts required for 2026. These shifts are designed to move organisations from perceived maturity toward demonstrable, auditable readiness.

1

Move from "visibility as a claim" to "visibility as proof."
N-tier visibility must be verifiable, continuously updated and auditable—not inferred or limited to crisis response.

2

Treat supplier engagement as core infrastructure, not a support activity.
Without scalable cooperation and data sharing, upstream mapping, ESG reporting integrity and early-warning capability remain fragile.

3

Rebuild data integrity as the centre of risk performance.
Focus shifts from more dashboards to fewer, higher-quality inputs: completeness, timeliness, validation, and consistency across systems.

4

Anchor governance narratives in evidence chains.
Under continuous scrutiny, teams need decision records that connect signal → assessment → decision → action → outcome, with clear traceability.

5

Reallocate investment toward structural bottlenecks, not incremental playbook expansion.
Diversification, buffers and near-shoring are now saturated levers. The next gains come from upstream intelligence and targeted supplier interventions.

6

Collapse decision latency: make "emergency speed" the default for priority suppliers and categories.
Pre-decision risk reviews must compress from days/weeks to hours through automation, integrated data and streamlined governance pathways.

7

Shift AI maturity from "faster alerts" to "better foundations + cross-category patterning."
AI advantage will come from combining validated data with pattern analysis that links viability stress to quality deterioration, ESG pressure and operational volatility—rather than producing more notifications.

If organisations close the confidence gap—by strengthening foundations and aligning governance expectations with demonstrable evidence—2026 becomes a year of improved defensibility and reduced disruption impact. If they do not, scrutiny will continue to intensify while confidence remains high on paper and disruptions remain a normal operating condition.

SCRM by Sphera

Sphera's Supply Chain Risk Management (SCRM) solution empowers organizations to future-proof their supply chains by providing real-time visibility, risk intelligence, and actionable insight for proactive mitigation strategies. With a combination of Artificial Intelligence (AI), Human Intelligence (HI) and Supplier Intelligence, Sphera helps innovative supplier chain leaders detect disruptions before they escalate; whether from geopolitical shifts, human rights violations, or supplier failures. Its end-to-end transparency ensures that organizations can assess risks across *N*-Tier suppliers, strengthening due diligence and compliance with evolving ESG regulations.

By leveraging data-driven decision-making, companies can transition from reactive crisis management to strategic resilience, optimizing sourcing strategies and minimizing exposure to high-risk regions. As supply chain uncertainty grows, Sphera's SCRM solution offers the agility and intelligence necessary to not just survive but thrive in an increasingly complex global market.

Learn more about Sphera at **sphera.com.**

Follow Sphera on **LinkedIn.**

Click here to arrange a consultation to find out more:
Get a consultation

sphera®