Leveraging ERM to navigate emerging tariffs and supply chain risks

AuditBoard

Table of contents

03 Introduction

04 Supply chain risks affected by heightened geopolitical volatility

06 The interconnected nature of supply chain risk

08 Proactive ERM strategies for addressing emerging supply chain risks

09 Forging resilient supply chains in a turbulent environment

Introduction

In the wake of the Trump administration's newly implemented tariff hikes on the U.S.'s key trading partners, including the United Kingdom, China, and Canada, organizations face an urgent need to strategize and fortify their supply chains. A 2025 supply chain risk report by global advisory firm WTW found 63% of businesses reported higher-than-expected supply chain losses, despite enhanced risk management efforts in recent years.

As organizations contend with geopolitical shifts amid inflation, increased raw material shortages, accelerating cybersecurity risks, and regulatory changes, a single supply chain risk can quickly cascade, impacting a company's strategic position, profitability, and public perception. 83% of risk professionals surveyed in Accenture's 2024 Risk Study report interconnected risks are emerging at a more rapid pace than before. Navigating this complexity requires an understanding of how supply chain risks can drive broader enterprise-wide issues — an area the enterprise risk management (ERM) function is uniquely positioned to help organizations address.

By providing a holistic view, ERM helps connect the dots between supply chain, vendor, cyber, and other enterprise risks amplified by tariffs and geopolitical uncertainty. This guide will explore the various risk domains affected by America's changing relationships with its trade partners and the distinct challenges of a stressed global market. We will then delve into ways in which ERM groups can enhance other risk teams' and owners' efforts in identifying, escalating, and responding to emerging supply chain risks with agility and speed.

Supply chain risks affected by heightened geopolitical volatility

Risk volatility continues to be a running theme as global supply chains ride the turbulence of tariff wars and shifting trade relationships. A new U.S.-UK trade agreement known as the Economic Prosperity Deal (EPD) provides insight and a likely template for future U.S. trade agreements, particularly for the auto industry, as well as beef, agriculture, and pharmaceuticals. The U.S.'s new 35% tariff on Canada may result in new Canadian tariffs on U.S. steel and aluminum imports this fall. Meanwhile, a temporary pause in U.S.-China retaliatory tariffs from August to November is providing only a brief respite amid ongoing trade negotiations. The outcomes of these negotiations will continue to alter supply chain risks in six key areas: **strategic, operational, financial, cyber, compliance, and reputational.**

Strategic risks revolve around fundamental shifts in how a business operates, its market position, and its long-term viability. Changes in supply chains due to tariffs and other geopolitical disruptions can greatly impact a business's strategy. Already, the U.S. has seen small businesses forced to close or consider shuttering their doors due to tariffs on Chinese imports.

Operational risks typically manifest as immediate, day-to-day challenges in moving goods, managing inventory, and maintaining production flow. Many organizations will see increased operational risks related to tariffs, such as supply bottlenecks created by increased costs and delays.

Financial risks are highly intertwined with strategic and operational shifts. The most obvious financial risk is the direct cost of new tariffs, which can immediately cut into profit margins, leading to liquidity risk. Businesses opting to diversify their supply chain to avoid tariffs (e.g., moving production from China to Vietnam or Mexico) also face significant financial costs, such as higher logistics costs, setup costs for new suppliers, increasing inventory holding costs, and loss of economies of scale.

Cyber risks, including third-party and Nth-party cyber threats, can affect your supply chain as well. Instead of exploiting targets directly, cyber attackers are often gaining access indirectly, via supply chains. The SANS 2024 Top Attacks and Threats Report cited more than 2,700 supply chain attacks in 2023, a disconcerting 2,600% increase since 2018. This is why, as businesses forge new relationships with third and Nth parties in response to operational shifts, effective third-party risk management is more important than ever.

Compliance risks related to supply chains are particularly dynamic and challenging. Trade negotiations between the U.S. and its economic partners are constantly changing the legal and regulatory framework for international trade, prompting companies to invest more in monitoring, documentation, and real-time adaptation to avoid costly penalties and operational disruptions.

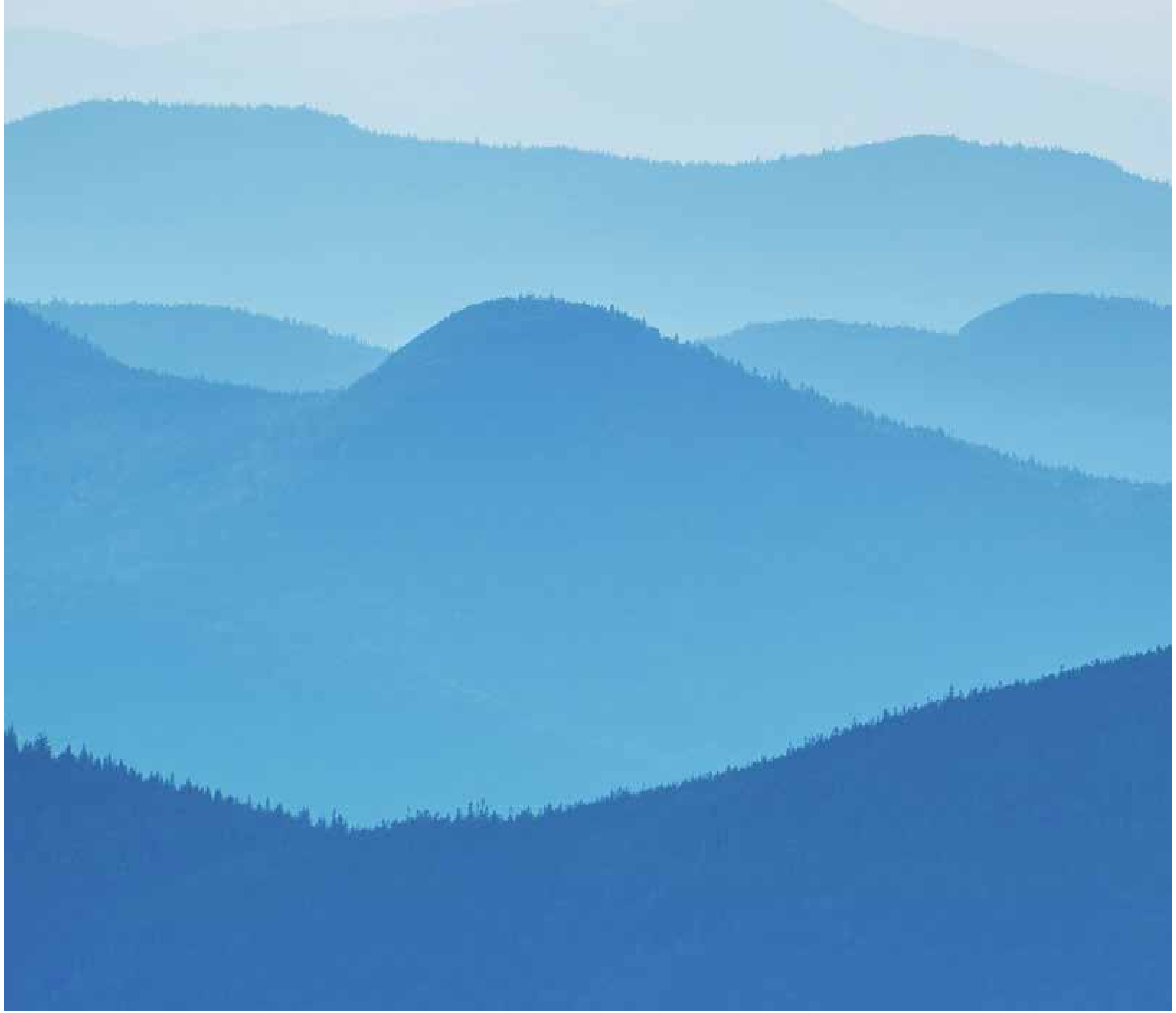
Reputational risks can arise from public perception shifts, ethical concerns, and the perceived "side" a company is on during trade disputes. An example of a reputational risk could be public backlash and boycotts against a company that passes tariff costs on to consumers, or a company forging new partnerships with unvetted partners or vendors as a result of tariffs.

The interconnected nature of supply chain risk

As geopolitical shifts create a new reality of interconnected threats, a single emerging supply chain risk can trigger a cascade of operational, financial, and reputational risks across an entire business.

For example, a new tariff (a financial risk) can trigger a chain reaction, forcing a company to find a new supplier (an operational risk), which could then lead to reputational damage if the new supplier has ethical issues. Similarly, a third-party cyber breach (a cyber risk) can disrupt production (an operational risk) and lead to significant financial and reputational harm for the main company.

Effective supply chain risk management therefore requires identifying these underlying drivers to understand their full, interdependent impact on the organization — **a process that ERM teams are specifically equipped to help support.** An overarching ERM program is vital for providing a holistic view of the business's risk landscape. While specialized risk groups and risk owners focus on specific domains like data privacy or cybersecurity, they often operate in silos, which can hinder risk visibility and make it difficult to efficiently address interdependent risks. ERM can offer a more well-rounded perspective on an emerging supply chain risk, highlighting important risk interdependencies and alerting the executive team of potential chain reactions that require attention. Thus, as trade negotiations proceed, businesses must have agile ERM processes in place to support their organizations in quickly adapting to emerging risk priorities.



Proactive ERM strategies for addressing emerging supply chain risks

In times of geopolitical volatility, the ability to plan and react quickly is the bedrock for supply chain resilience and, in turn, organizational resilience. The following are key considerations for building agility, accuracy, and speed into your ERM program to help proactively identify, escalate, and respond to emerging supply chain risks.

1. Schedule regular risk calibration exercises with your executive team. Complement your risk assessments with regular risk calibration exercises to keep your enterprise risk universe current. Aim to hold these sessions with your executive team three to four times a year to stay on top of emerging risks and align risk management with business objectives and strategy. Before each meeting, research and reconcile industry trends on emerging risks affecting your industry to identify which emerging risks can significantly impact your enterprise risks.

ERM Tip

Frame the conversation around risk interconnection. When facilitating risk calibration meetings, highlight how the emerging risk impacts your existing enterprise risks, rather than treating the risk as a standalone issue. For instance, new tariffs aren't just an emerging risk; they can be a driver of supply chain and operational risks. By facilitating this structured process, ERM can ensure emerging insights are quickly fact-checked and escalated to secure executive buy-in.

2. Focus on identifying and understanding the root cause. It's not enough to simply identify an emerging risk. To derive value from any risk assessment or risk calibration exercise, identifying the correct root cause is key to formulating actionable recommendations. When interviewing your chief supply chain officer, inquire about the underlying drivers behind their identified risks. This conversation and your resulting insights are crucial for developing an effective plan of action, such as scheduling an internal audit or creating a management action plan to address the root cause.

3. Proactively update your vendor risk assessment results. Traditional vendor risk assessments, often conducted during selection and onboarding, typically focus on direct concerns like data privacy (e.g., GDPR compliance) and cybersecurity. However, in today's volatile global landscape, it's crucial to proactively update these assessments to gain deeper visibility into your entire supply chain. This means going beyond your immediate vendors (third party) to understand the risks posed by their suppliers, and even their suppliers' suppliers (fourth party to Nth party). Geopolitical shifts and new tariffs can significantly impact these extended vendor networks, creating hidden vulnerabilities. By proactively reassessing these deeper relationships, you can identify critical gaps and risks, allowing you to prioritize efforts and strengthen your supply chain. The ability to perform these comprehensive vendor risk assessments with agility and efficiency is therefore paramount for maintaining supply chain resilience.

Tech Tip

AuditBoard's vendor risk assessment feature enables risk teams to build and send out vendor risk assessments all in one place, with configurable questionnaire capabilities for evergreen scenarios like new tariffs and a vendor library where all your vendor data lives.

4. Leverage scenario planning to strategically prepare for new challenges or disruptions. This involves simulating potential disruptions to systematically identify vulnerabilities and develop robust contingency plans. Effective scenario planning requires a structured approach: identifying plausible disruptions, developing and rigorously testing detailed "what-if" scenarios, assessing the organization's current resilience capabilities, and then formulating response strategies. Regularly reviewing and updating these scenarios is critical to their ongoing efficacy. Embedding a scenario planning framework into your ERM program can help optimize decision-making under pressure and bolster business continuity during crisis.

Proactive ERM strategies for addressing emerging supply chain risks

5. Empower your frontline risk owners to proactively report emerging risk events and data. These individuals are uniquely positioned to observe the immediate impacts of new tariffs and trade developments, as they are closer to those impacts than your central risk management teams. Therefore, empowering the business to proactively report emerging risk events and data is essential to ensuring continuity in your organization's risk universe. Implementing a direct reporting mechanism from the business to risk management channels helps ensure vital information is rapidly escalated to the second line. This also fosters a shared understanding of risk across the organization, promoting consistent risk management and empowering employees to make risk-aware decisions.

Tech Tip

AuditBoard's intuitive, easy-to-use risk event intake form enables risk owners to report risk events, with a workflow that connects the information back to your risk universe. This helps stakeholders achieve a better understanding of the organization's risk health.

6. Revisit your organization's risk appetite and tolerance scores. In light of new tariffs and negotiation outcomes, it is essential to revisit your organization's risk appetite and tolerance scores. These scores are not static; instead, they must evolve to accurately reflect the "new reality" shaped by ongoing trade negotiations and geopolitical shifts. Reassessing them provides a clear, up-to-date framework for deliberate decision-making, enabling calculated trade-offs (e.g., accepting more reputational risk for critical financial stability) and optimizing resource allocation.

Tech Tip

AuditBoard's risk appetite capability enables risk teams to establish how much risk their organization is willing to accept, determining what is within or outside their tolerance — this allows stakeholders to track their risk scores in real time, contextualize the significance of the risk score, and quickly report on changes. Risk teams can also temporarily adjust their risk appetite in light of new challenges, enabling them to see how this change reflects in their risk environment.

7. Implement real-time risk monitoring and alerting to keep pace with today's rapidly changing global landscape. Up-to-date monitoring of your supply chain risks is critical for swiftly acting on new information. Real-time insights are essential for informing your action plans, whether that means updating vendor risk assessments, reassessing risk appetite and tolerance scores, or escalating a high-priority strategic risk directly to the executive team for immediate attention.

Tech Tip

In AuditBoard, audit, risk, and compliance teams can collaborate in a single source of truth, surfacing real-time insights across teams, whether that is updates to issues, action plans, risks, controls, or audits. This increases overall transparency and visibility, enabling teams to escalate issues quickly and empower leadership to make risk-aware, data-driven decisions.

8. Establish a common risk language across the organization. By facilitating the creation of a common risk language and risk ranking methodology for use across the business, ERM can help drive improved emerging risk visibility and prioritization. A connected risk platform centralizes risks and controls in a single source of truth, ensuring a consistent, unified risk language across departments. By integrating risk data from different teams, an organization can bring together diverse insights and data, ensuring a common understanding of risk that no single department could achieve alone.

Tech Tip

In AuditBoard, a risk hierarchy helps provide a structure where granular risks from different departments can roll up into enterprise-level risks, allowing leaders to see how individual risks contribute to the overall risk profile of the organization.

Forging resilient supply chains in a turbulent environment

The U.S.'s increased tariffs and ongoing trade negotiations have undeniably reshaped the global trade landscape, demanding a proactive approach to supply chain management that transcends traditional risk considerations. To thrive amid this uncertainty, businesses must empower frontline risk owners, continuously re-evaluate their risk appetite, update vendor assessments for deep visibility, and leverage real-time monitoring and scenario planning. Thanks to its enterprise-wide perspective, ERM can help connect data and expertise from various risk groups — along with audit, cybersecurity, and compliance teams — to provide a holistic view of supply chain risks. This approach helps the organization focus on risk interconnections, ensuring emerging threats are not missed and resources are strategically allocated for a coordinated response. Ultimately, a truly successful ERM program is one that not only identifies risks but actively responds to and mitigates them, enabling businesses to build resilient supply chains capable of adapting to any future disruption.

About the authors

Claire Feeney

Senior Product Marketing Manager, AuditBoard

Claire Feeney is a Senior Product Marketing Manager at AuditBoard focused on ESG and RiskOversight. In her role, she helps support organizations in transforming their enterprise risk management and sustainability programs. Prior to joining AuditBoard, Claire worked in product marketing at OneTrust, VMware, and Infor.

Hayley Burger

Senior Product Solutions Manager, AuditBoard

Hayley Burger is a Senior Manager of Product Solutions at AuditBoard, where she helps organizations streamline their audit, risk, and compliance programs through technology. Hayley began her career in PwC's Risk Assurance practice where she specialized in Internal Audit, Forensic Accounting, Risk Management, and Compliance. She also worked at Raytheon Technologies on their Forensic Audit and Compliance Team. Hayley is a Certified Public Accountant (CPA) and Certified Fraud Examiner (CFE).

About AuditBoard

AuditBoard's mission is to be the category-defining global platform for connected risk, elevating our customers through innovation. More than 50% of the Fortune 500 trust AuditBoard to transform their audit, risk, and compliance management. AuditBoard is top-rated by customers on G2, Capterra, and Gartner Peer Insights, and was recently ranked for the sixth year in a row as one of the fastest-growing technology companies in North America by Deloitte.