

Industry Agenda

Building Resilience in Supply Chains

An Initiative of the Risk Response Network
In collaboration with Accenture

January 2013



Executive Summary

Global supply chains and transport networks form the backbone of the global economy, fuelling trade, consumption and economic growth. Disruptions to supply chains can prove costly, as highlighted most recently by Hurricane Sandy. According to research conducted by Accenture, significant supply chain disruptions have been found to cut the share price of impacted companies by 7% on average.

The World Economic Forum's Supply Chain Risk Initiative first started exploring systemic risks and vulnerabilities to global supply chains and transport networks in 2011. The initiative's phase I report, *New Models for Addressing Supply Chain and Transport Risk*, launched at the World Economic Forum Annual Meeting 2012 in Davos-Klosters, examines the systemic supply chain risk landscape and the possibility of these risks causing serious disruptions to global supply chains. It highlights the need to shift focus from reactive to proactive risk management. At the same time as the launch of this report, the US government launched its Strategy for Global Supply Chain Security, calling for a global multistakeholder dialogue to effectively safeguard supply chains.

Throughout 2012, concerns have remained about external threats to supply chains (such as natural disasters and demand shocks) and systemic vulnerabilities (such as oil dependence and information fragmentation). Additionally, growing concern around cyber risk, rising insurance and trade finance costs are leading supply chain experts to explore new mitigation options. Accenture research indicates that more than 80% of companies are now concerned about supply chain resilience.

This report, **Building Resilience in Supply Chains**, developed during phase II of the initiative, explores government and industry sector views on systemic supply chain risks and building a resilience framework to manage them. The report findings are based on expert level workshops and data gathering throughout 2012. Notable differences in perspectives stem from government responsibility for public security and long-term risks compared to industry's focus on ensuring that supply chains work effectively on a day-to-day basis. Differences in regional perspectives, attributed

to differences in disruption histories and growth expectations, also point to the need for a harmonized resilience framework. However, the top risk concerns in Europe, North America and Asia in 2012 showed little change from the previous year apart from a sharp rise in concern about extreme weather. Of emerging non-traditional risks, cyber risk is perceived to have the greatest implications for supply chains.

The workshops and dialogues have produced suggestions on how to ensure that business and government approaches to building resilience are complementary. Three "must have" requirements have emerged from our analysis: the need for a common risk vocabulary; improved data and information sharing across supply chain actors; and building greater agility and flexibility into resilience strategies. This led to the creation of an overall blueprint for resilient supply chains based on four core components: partnerships, policy, strategy and information technology (IT). This blueprint underpins a set of recommendations to guide multistakeholder engagement.

Systemic risks have global geographic scope, cross-industry relevance, uncertainty as to how and when they will occur, and high levels of economic and/or social impact requiring a multi stakeholder response. These risks are also magnified by the way supply chain systems are configured; and cannot be mitigated by individual actors. Risk management must be an explicit but integral part of supply chain governance. To achieve this, several steps are recommended:

- Institutionalize a multistakeholder supply chain risk assessment process rooted in a broad-based and neutral international body
- Mobilize international standards bodies to further develop, harmonize and encourage the adoption of resilience standards
- Incentivize organizations to follow agile, adaptable strategies to improve common resilience
- Expand the use of data sharing platforms for risk identification and responses

