



Advancing Supply Chain Risk Management

For organizations looking to improve operational performance and better manage risks in an unpredictable world, a supply chain risk management program is critical for success.

Risk events such as pandemics, cybersecurity attacks, geopolitical uncertainty, and climate-related weather incidents are driving organizations to review and, if necessary, overhaul their existing supply chain risk management (SCRM) strategies. Add to that increased competition, third-party complexity, supply chain continuity challenges, new business models, and changing regulations, and it's clear that a robust SCRM program is essential to helping organizations improve operational performance and more effectively manage risks.

How does your organization maintain a resilient, stable supply chain in the face of extensive risk exposure?



Competition Risks

- Regulations
- New competitors
- Increasing costs
- Reputational costs
- Stranded assets



Business Risks

- Customer expectations
- Technology obsolescence
- Regulatory risks
- Code of conduct compliance
- Fraud, bribery, and corruption
- Transparency
- Privacy



External Risks

- Supply chain disruption
- Climate change/ environmental
- Cyber threats
- Privacy
- Third-party risks
- Digital, robotics, AI, crypto
- Pandemics
- Weather incidents
- Security/terrorism
- Fraud, bribery, corruption
- Counterfeiting, product tampering

Key Challenges Organizations Face

Organizations are faced with significant challenges due to volatile, unpredictable, and vulnerable supply chains.



Supply Chain Risk Management

SCRM is one key element within a broader risk resilience model. Other areas include compliance risk management, cyber risk management, and operational risk management. These elements coexist within the enterprise risk management, pandemic, and sustainability environments. A robust, formal SCRM program allows an organization to execute strategy and improve operational performance during times of supply chain normalcy—and supply chain disruption.

This is accomplished by:

- **Supporting** a more resilient, predictable supply chain process.
- **Knowing** key entities, processes, materials, and actors in various supply chain tiers.
- **Understanding** the risks from these entities, processes, materials, and actors.
- **Addressing** proactively those risks to prevent operational disruptions.
- **Empowering, enabling, and equipping** plant managers with the tools, knowledge, and methods to more effectively manage local supply chain risks.

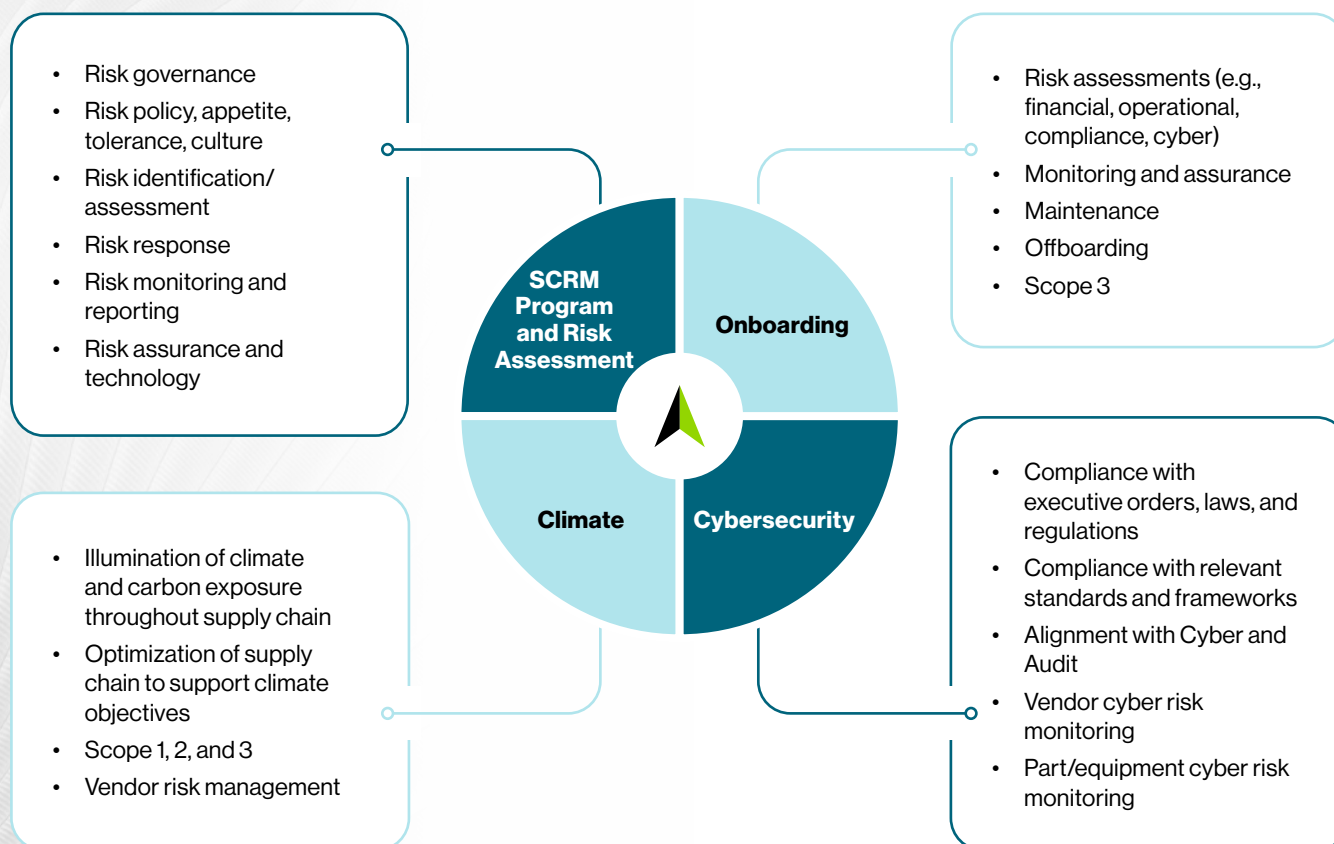


Key Imperatives

- **Build** a formal SCRM program, based on enterprise risk management (ERM) principles. Our approach includes the following dimensions: risk governance and oversight, risk appetite, risk identification and assessment, risk response, risk reporting/monitoring, risk assurance, and the use of risk technology.
- **Illuminate** and map the supply chain to identify the parties involved, including suppliers, vendors, manufacturers, brokers, freight forwarders, and other service providers—as well as the suppliers' suppliers. We help clients create a “map” that is as detailed as possible, showing the entire supply chain for the system, component, or product, often to the fifth tier or below.
- **Conduct** supply chain risk assessment to determine the risk of third parties with controlling or influential interests, along with their location and associated activity. We work with clients to develop a customized set of risk factors to perform risk assessments on new or existing supply chain providers.
- **Perform** open-source, commercial due diligence investigations to identify potential threats. Using analytical tradecraft and commercial best practices, our due diligence reviews help identify and verify factors such as beneficial ownership, business reputation, financial well-being, commercial practices, related business activities, business partners, disputes or litigation, USG contracts, relationships with foreign governments or individuals, sanctions or watchlist data, and civil or criminal investigations.
- **Assess** the strategic impact of potential threats and present results in analytical or other types of reports to the client—specific to its supply chain. In some cases, there may be nothing of concern; in others, we may find adverse or even high-risk information, such as connections to a hostile foreign head of state, cyber breaches, counterfeiters, substandard parts, or other issues of financial or quality control concern.
- **Provide** mitigation and remediation recommendations to address vulnerabilities or other deficiencies and threats and work with our clients to implement changes as necessary. For example, we have recommended to some clients that they conduct penetration testing, change suppliers, perform continuous monitoring, enhance common minimum standards, carry out surprise inspections or periodic reassessments, provide referrals to law enforcement or intelligence, or issue warnings about or prohibit certain vendors.
- **Monitor** critical and sensitive components and entities continuously. This is increasingly necessary and should be the standard...across the most sensitive parts of key national security- and business-related supply chains. One-time reviews or “snapshots” are no longer adequate. Comprehensive, continuous monitoring and evaluation of suppliers is necessary to inform stakeholders of changes to risks that may arise on an almost daily basis.
- **Evaluate** the vendor management system with Sourcing/Procurement. Ensure it is consistently used across the organization, includes a centralized repository, and possesses the following functionalities: vendor search, invitation, self-service/registration, profile qualification, onboarding, maintenance, offboarding, assuring/testing, performance management, alerts/notifications, reporting/dashboards, security, and workflow.
- **Review** the contract management system with Legal. Ensure it is consistently used across the organization, includes a centralized repository, and deploys the following functionalities: request and intake, search capabilities, contract clauses, template libraries, a hierarchy of all master agreements/amendments/orders, redlining/approval, electronic signature, and maintenance.
- **Orchestrate** the supply chain. Individual SCRM functions (e.g., sourcing, supplier management, third-party risk management, asset protection) need to be effective individually, orchestrated collectively, and integrated with strategy, planning, finance, operations, and other key functions to further create, preserve, and realize value.
- **Drive** organizational integration. SCRM, cybersecurity, ERM, and other crucial elements of the supply chain often happen in isolated pockets throughout organizations. We help break down internal silos and pave the way for information-sharing and collaboration with internal and, where appropriate, external stakeholders.

SCRM Areas of Focus

Here are the areas your SCRM program should focus on:



The Value of a Guidehouse SCRM Program

A robust SCRM program provides the following benefits:



Why Guidehouse

Guidehouse has the supply chain risk management capability, experience, skills, tools, data, and discretion to provide government and industry clients with the ability to develop insights into the business entities and individuals in their vendors' supply chains.



Experience

- **Technical Experience.** Guidehouse has extensive experience in evaluating and enhancing SCRM programs to assist our clients in executing their strategies, improving performance, and reducing risk.
- **Industry Experience.** Guidehouse brings substantial experience in the industries that we serve. Many of our consultants have joined us from senior roles within those industries.



Track Record

- **Proven Track Record of Success as a Trusted SCRM Advisor.** Guidehouse has served as the trusted advisor to numerous private and public sector organizations.
- **Global Reach.** With more than 50 offices around the world and over 8,000 consultants, Guidehouse can provide support for supply chain risk management worldwide.



Data-Driven

- **Data-Driven Products Tailored to Client Needs.** Our subject matter experts leverage proprietary tools and data, open-source and subscription databases, and commercial best practices to deliver insightful and actionable research products and modernize supply chain risk management practices.



Client- and Quality-Focused

- **Best-in-Class Resources, Research, and Subject-Matter Expertise.** We help our clients create scalable, innovative solutions, solving their challenges and preparing them for future success.
- **Uncompromising Quality.** As the first and only large professional services firm to receive the Malcolm Baldrige National Quality Award, we pride ourselves on the quality of our work, products, and impact.

Jason Dury

Director, Cybersecurity / jdury@guidehouse.com

Derrick Sturisky

Director, Cybersecurity / dsturisky@guidehouse.com

About Guidehouse

Guidehouse is a leading global provider of consulting services to the public sector and commercial markets, with broad capabilities in management, technology, and risk consulting. By combining our public and private sector expertise, we help clients address their most complex challenges and navigate significant regulatory pressures, focusing on transformational change, business resiliency, and technology-driven innovation. Across a range of advisory, consulting, outsourcing, and digital services, we create scalable, innovative solutions that help our clients outwit complexity and position them for future growth and success. The company has more than 12,000 professionals in over 50 locations globally. Guidehouse is a Veritas Capital portfolio company, led by seasoned professionals with proven and diverse expertise in traditional and emerging technologies, markets, and agenda-setting issues driving national and global economies.

For more information, visit: www.guidehouse.com

Web: www.guidehouse.com/cybersecurity

 [Twitter.com/GHTechSolutions](https://twitter.com/GHTechSolutions)

 linkedin.com/company/guidehouse

© 2022 Guidehouse Inc. All rights reserved. W397500. This content is for general informational purposes only and should not be used as a substitute for consultation with professional advisors. This publication may be used only as expressly permitted by license from Guidehouse and may not be otherwise reproduced, modified, distributed, or used without the express written permission of Guidehouse.