



**Cut Costs and Deliver Innovation? Say
YES to Both**

What is supply chain risk management?

Supply chain risks are an ever-present concern for global enterprises. Unanticipated vulnerabilities can lead to increased costs and unhappy customers. To mitigate these and other issues, supply chain managers and stakeholders around the world are turning towards *supply chain risk management (SCRM)*.

The term *supply chain risk management* refers to the processes, strategies, and tools designed to identify any and all dangers that may potentially affect supply chains. After pinpointing and evaluating these dangers, stakeholders further rely on SCRM strategies to mitigate and recover from supply chain risks. This helps to ensure the uninterrupted flow of goods and materials to those businesses and customers who depend on them.

Supply chain activities cover everything from product development, to sourcing, production, and logistics, as well as service delivery and information systems needed to coordinate these activities.

Benefits of supply chain risk management

Effective supply chain risk assessment and management can impact organizations in a number of positive ways. These include the following advantages:

- Reducing profit loss
- Ensuring peak efficiency in production, fulfillment, and delivery
- Improving speed and effectiveness in responding to emergent situations affecting the supply chain
- Maintaining compliance and keeping up with regulatory issues

- Creating reliable processes for handling unexpected interruptions in the supply chain
- Protecting brand reputation
- Increasing competitive advantages
- Improving customer satisfaction

What is the supply chain risk management process?

While many consumers take for granted that products will naturally be ready and available whenever they need them, the reality is that supply chains are extremely fragile. Much like holiday lights that fail when a single bulb burns out, the risk of disruption exists with every supplier and nearly every activity at every level of the supply chain.

The supply chain itself can be made up of as few as one supplier, or potentially thousands. For example, a manufacturing company may need a third party to supply the parts, a fourth-party supplier for packaging, and multiple fifth-party suppliers to handle labeling or other aspects. Likewise, an organization may provide the workforce to deliver a service, but use a third-party credit processing company, who in turn uses a fourth party for credit checks.

Reliable, timely delivery depends on each of these suppliers; if any fail to deliver as expected, the desired service or product may not reach its intended destination on time and at the right cost.

The SCRM process first identifies the parties within a supply chain, emphasizing the most critical suppliers. These suppliers are assessed for regulatory compliance, as are the fourth- and fifth-party suppliers that provide them with goods and services. Each supplier is reviewed for insights into past performance and potential risks. Any issues that are discovered are addressed immediately and resolved as quickly as possible. Finally, real-time

dashboards and up-to-date reports allow internal stakeholders to continue monitoring the suppliers and the supply chain for any emerging changes.

Put more simply, the SCRM process consists of four specific steps:

Identify

Catalog which risks could potentially impact your supply chain, as well as where in the chain they may be found.

Quantify

Estimate the possible operational, financial, and reputational impact these risks could have on your business.

Mitigate

Construct or identify relevant strategies and tactics to offset the negative impact of specific forms of supply chain disruption.

Respond

Determine how quickly you would be able to respond to a disruption, and how much time it would take for your business to recover from the event.

What are common forms of supply chain risk?

It can be difficult to fully account for every possible supply chain risk. Every step along the way could be impacted by a number of potential issues, including operational failures, cyber attacks, disasters, pandemics, regional instability, economic downturn, and more. And unfortunately, a supply chain is only as strong as its weakest link.

With that in mind, many supply chain managers group risks together into six specific categories:



Cyber

Suppliers that rely on modern technology may fall prey to cyber attacks or issues related to not complying with cybersecurity requirements. In both cases, these risks may result in damage to the supplier and the supply lines, and indirectly cause harm to your business.

Financial

Market volatility, bankruptcy, regional economic downturn—these can all pose a serious threat to a supplier's financial health. When suppliers have to cut costs, reduce routes, increase prices, or even close their doors for good, the businesses that depend on them end up suffering.

Geopolitical

When governments are replaced, wars erupt, or tariffs change unexpectedly, supply chains may be affected. This can mean something as minor as short delivery delays or small cost increases, or may result in complete disruption and even loss of purchased goods and materials.

Man-made

Fires, explosions, and other risks that come as a result of the action or inaction of an individual or group can likewise cause serious problems along the supply chain. Additionally, suppliers sometimes choose not to report these disruptions, forcing the businesses that depend on them to actively monitor the supply chain for man-made risk events.

Natural

Sometimes, the planet and the environment themselves seem like they're trying to disrupt essential supply chains. Natural disasters, such as earthquakes, hurricanes, severe snowstorms, etc., can emerge with little to no warning, and throw global supply chains into complete disarray.

Reputational

It's said that you're judged by the company you keep. This can certainly be true in terms of supply chains, where the actions of suppliers can create reputational damage that may be passed on to your business. Issues related to corporate social responsibility and compliance are the most common.

What are the challenges of supply chain risk management?

As the internet developed and became the primary environment for managing supply chains, complex digital ecosystems began to emerge. Gone are the days when companies worked almost exclusively with local suppliers and within linear supply chains; now your suppliers and competitors may be on the other side of the world.

At the same time, consumer expectations have been bolstered by the near-limitless accessibility and selection offered by internet-based retail. Competition is fierce, customers are quick to switch brands, and risks have expanded along with supply chain complexity.

To counter these trends, businesses must be faster, cheaper, and higher quality, and that means that the supply chain has to improve as well.

To do so, organizations have to overcome three major challenges:

Transparency

The number of potential suppliers that may contribute to a single product can be almost unfathomable. Supply-based transparency—the ability to accurately identify what suppliers are contributing and at what stages—is a major challenge for supply chain managers

Scoping

It can be challenging enough to fully account for the number of possible risks that face your supply line, but even more difficult is correctly estimating the probability, severity, and impact of each risk. Without a detailed sense of the scale and scope of possible risks, it may be impossible to quantify and mitigate emergent issues.

Proprietary Data

Not every supplier is willing to share vital data. This can create blind spots within the supply chain, harming visibility and limiting access to information that may be vital to SCRM.

While these challenges may make effective SCRM difficult, the right tools can help make up the difference. ServiceNow Vendor Risk Management provides automation, reporting, and remediation solutions, to help ensure that your vital supply chains keep moving.