

You are the Weakest Link

This feature is Part 4 of the Third-Party Management Illustrated Series presented by OCEG and Compliance Week. To download a copy of the illustration on the facing page fold-out and for prior illustrations in OCEG's GRC Illustrated Series, please go to www.complianceweek.com and select the "GRC Illustrated" by selecting the "News" pull-down menu, then choosing "Topics."

By Carole Switzer

We talk a lot today about the growing complexity of supply chains in the global economy.

With an almost uncountable number of parties (or links if you will) in many undefined and ill-managed supply chain relationships, the chance of significant or fatal weakness seems immeasurable. The complexity presented by the number, nature, and structure of these relationships is exacerbated by uncertainty about risks that each may present; which may cause disruption in the supply chain, economic loss, or reputational damage. And yet, complexity is necessary to compete.

So how do you find the proverbial weakest link in a supply chain? How do you reduce the uncertainty that contributes to complexity in a negative way without sacrificing the structure that satisfies your supply chain needs?

I recently read a whitepaper entitled "Top 5 Reasons for Supply Chain Complexity," published by Ontonix (a firm that specializes in measuring complexity in business operations), which lists the key factors as: numerousness, variety, inter-connections, opacity, and dynamic effects. While some of these seem self-explanatory, even the scope of the variables within each factor can be challenging to define. For example, the factor of "numerousness" refers not only to the number of suppliers, but also to variables such as number of parts, available inventory levels, orders completed, and other items that can be counted and that have an effect on supply chain needs. As noted in the whitepaper, the inter-connections between the many influencing variables are constantly changing in ways that increase complexity even more.



Switzer

But the factor that interests me most is the one that the whitepaper calls "opacity," for this is something that risk managers can and must address. Opacity is the flip side of transparency. And to gain transparency, and thus a clear view of supply chain risks as they grow and change, requires thoughtful management of information about all of the contributors to complexity in a structured way that enables analysis.

In too many organizations, that struc-

Even worse, many organizations believe they are taking a mature approach to supply chain management because they are focusing on optimization.

tured system of information management, measurement, and analysis simply does not exist. Even the view of whom and what is part of each supply chain, and the types and ranking of risks presented by each such "link," is opaque. There is no unified approach to identifying risks and mapping them to each participant, and there is no method for determining how many relationships a given supplier has with various parts of the organization. Too many organizations can't see the cumulative or domino effects that a weakness or realization of risk in one link of a supply chain may have on them.

This can lead to significant disruption if, for example, there is too much reliance on one supplier and that source has a high level of risk that comes to pass and causes problems. This may be the case even when there are multiple sources, if the risks they face aren't properly analyzed so that consolidation of risk is evident. We saw for example, where companies may have had multiple suppliers but they were all located in the path of Hurricane Katrina.

Even worse, many organizations believe they are taking a mature approach to supply chain management because they are focusing on optimization. This is a management technique that seeks to better refine understanding of the true needs, in terms of timing and number, for receipt

of parts for example, so that inventory is kept at exactly the right level with neither too little or too much. While this is helpful in terms of managing things like warehouse space and accounts payable levels, if the potential of risk realization is not taken into the mix to ensure contingency planning, optimization can leave the organization in a vulnerable state.

Another analysis that is often ignored regards the capacity of selected suppliers. For example, during the BP spill disaster

in the Gulf of Mexico, the media reported that most (if not all) of the oil rigs in the region were supported for disaster response by the same third party. Just how well could that company respond if multiple issues arose at the same time? How many supply chains would be disrupted then?

I would argue that the overall lack of insight is grounded in a failure to build and support an integrated supply chain risk-management capability with clear assignment of duties, provision of standard processes and training, and technology that allows for real in-depth monitoring and oversight. The failure to gain and use timely information inevitably challenges the organization's ability to compete.

In these instances, the answer to the question of who is the weakest link is clear. In the words of Anne Robinson, the dour game show host, "You are the weakest link." And just like the contestants on her show, who were dropped through a hole in the floor as she dismissed them with these words, your organization will fall out of the competitive landscape if you aren't better prepared to know the answers you need to succeed. ■

Carole Switzer is the co-founder and president of OCEG, a non-profit think tank that develops standards and guidance to help organizations achieve Principled Performance—the reliable achievement of objectives while addressing uncertainty and acting with integrity. www.oceg.org.

DEVELOPED BY  WITH CONTRIBUTIONS FROM   

The Building Blocks of Supply Chain Risk Management

Supply chains present almost unimaginable complexity, often having an undefined and ill-managed number of levels with various parties involved across multiple supply chains. Each of these "links" in the chain presents a range of risks. The challenge of effectively managing the ever-changing and often cumulative risks in thousands of continually shifting supply chains can be overwhelming. Having a well-developed capability with appropriate technology, processes, and assignment of responsibilities is essential.

BUILDING BLOCKS

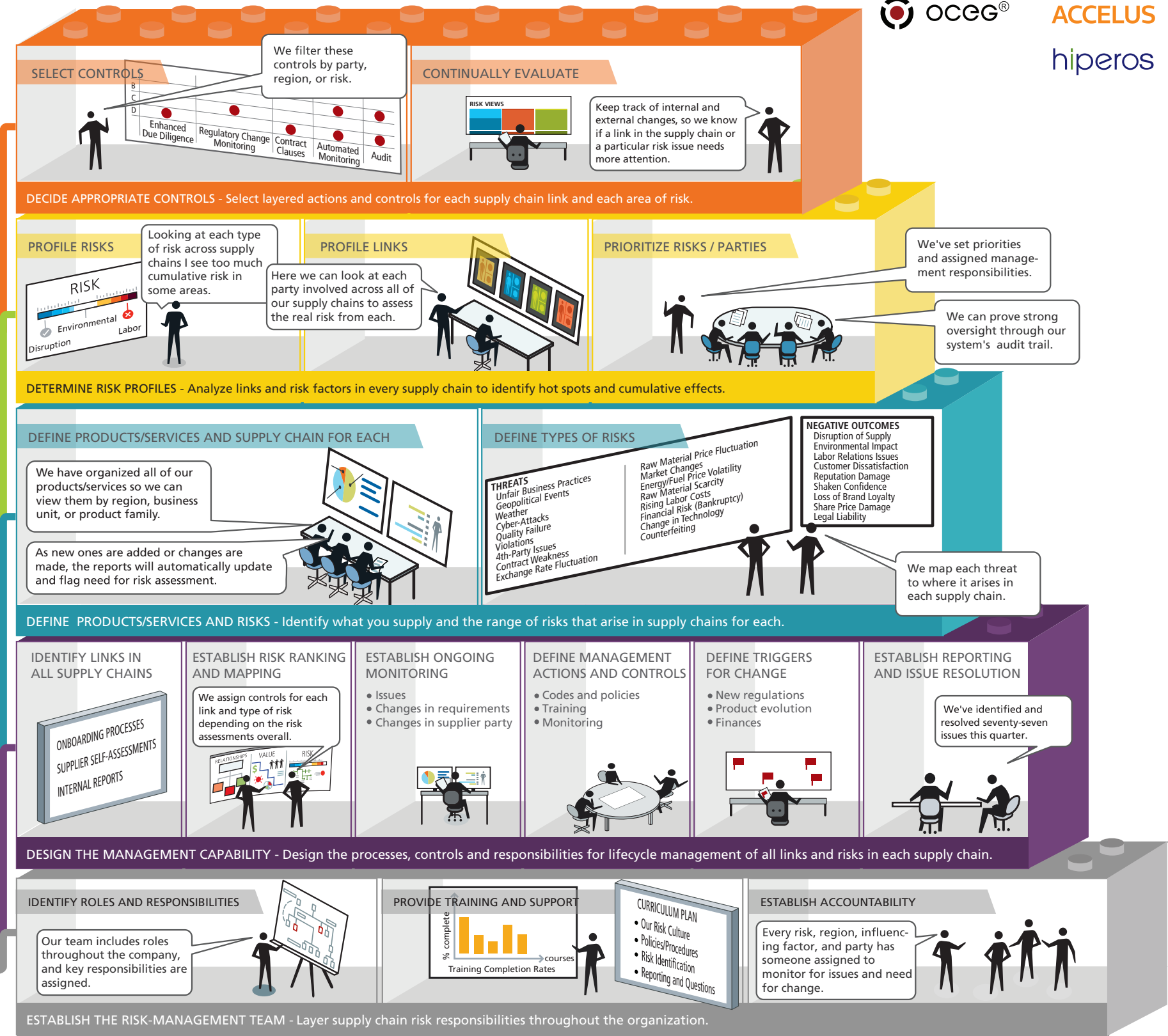
A strong supply chain risk management capability is built on a solid foundation of design and knowledge. Set the building blocks of that foundation in place and connect them in a unified technology system to ensure effective lifecycle management.

KEYS TO SUCCESS

- Identify every link in every supply chain, the roles they play, and the risks associated with them.
- Use a code of conduct, policies, and training to promote awareness of supply chain risk and understanding of required conduct for both employees and parties in the supply chain.
- Select the right technology platform and due diligence partners to build risk intelligence.
- Identify, evaluate and manage risk consistently across and throughout all supply chains, using a standard approach to risk ranking and prioritization.
- Continually monitor and evaluate the supply chain risk management capability.

COMMON MISTAKES

- Addressing only a small subset of parties in the supply chain, and then failing to manage even these based on risk ranking
- Failing to do business continuity planning
- Having inadequate communication between management and personnel involved
- Allowing activities that reduce supply chain transparency
- Not considering consolidated impact



[AN OCEG ROUNDTABLE]

Managing Supply Chain Risk

SWITZER: Let's start with what we mean by supply chain—who and what make up a supply chain?

PATTERSON: While our customers across different industries define “supply chain” in many ways, ultimately they are concerned with the inter-related dependencies of materials, products, and services that allow them to deliver their goods and services to their customers. For our customers in the oil and gas sector, this can mean the 30 or more different entities involved in moving equipment from a manufacturing location in the United States to an oilfield in the Middle East—think freight forwarders and customs brokers. Our banking customers are more concerned with service delivery, increasingly dependent on technology providers and concerns about consumer impact. In food manufacturing, our customers think about availability and traceability.

WYLIE: Often the term “supply chain” is used in the context of tier 1 suppliers, but there is much more to it. We are really talking about the “value chain” and not one, but multiple chains each consisting of multiple layers. It's the movement of materials as they flow from their source to the end customer—not only raw materials, but labor, utilities, management, and all inputs to the product or service. It's made up of the people, activities, information, and resources involved in moving a product from its supplier to its customer. Although this definition may sound

complex, effective management of a supply chain for some organizations can prove even more so. Value chains are multi-tiered, and a problem in one area can quickly have a ripple effect up and down the chain.

KEVERN: I agree the traditional term “supply chain” does not nearly reflect the complex third, and fourth and fifth, and so on party relationships we are seeing today. In recent years, Dell has significantly shifted from computer hardware manufacturer to provider of end-to-end technology solutions in virtually every corner of the globe. At the same time, our sales model has shifted from primarily direct to include channel. Consequently, our “supply chain” has grown from suppliers of product components our company manufacturers to include multi-tier channel partners, resellers, distributors, consultants, agents, vendors, and other business partners.

SWITZER: As we expand beyond concern for efficiency, what are some critical aspects of supply chain risk management today?

WYLIE: Supply chain resilience and minimizing costs are two goals that frequently conflict, and that's a challenge. Years back, Whirlpool decided to outsource the production of dishwasher water seals to a Chinese supplier which totalled a saving of over \$2 million annually. But soon after the arrangement was made, the Chinese supplier changed

to a different rubber supplier, raising a multi-tiered effect as previously mentioned. The seals made from this new rubber leaked in dry climates, causing a failure rate of nearly 10 percent, reputational damage, and revenue loss. So, often it takes a crisis to motivate action and change the way in which we mitigate supply chain risk. Every decision made to increase resilience or reduce costs should be viewed through a risk lens to determine how the decision will modify the company's risk profile.

KEVERN: The main concern companies face today is damage to brand or reputation brought forth by a rogue third-party employee or result of poor business practices. There is also a balance between refraining from exercising too much control over third parties and providing direction and oversight necessary for adequate assurance. For this reason, it's important to establish controls at the entry points into an organization. Dell deploys third-party due diligence to determine whether a given supplier, vendor, or sales partner has the same ethical and compliance values and principles as Dell. Companies that do not share this philosophy are not invited to be part of the Dell family. Changing the way companies view success in the supply chain is a shift in thinking, and more and more companies are seeking the right business partners. Meaning, business partners who share a passion for winning and demonstrated commitment to ethical business practices. This concept applies

throughout the duration of the relationship. Meaning, if a distributor sells to an embargoed country or a logistics service provider is engaged in bribery, established processes to off-board as well as prevent re-entry are critical. This proactive management of the supply chain helps mitigate risk of a future catastrophic event.

PATTERSON: The challenge for so many of our customers is that traditional supply chain management only gives them visibility to their immediate tier 1 with whom they contract. So visibility to tier-N—across what is now a value chain, versus only a supply chain, is limited. Our increasing dependence on global, cross-border flows is introducing additional elements to supply chain management. Traditional supply chain concerns of cost, quality, timely delivery, IP protection continue to be paramount. However today's supply chain managers are also being tasked to understand and address broad risk concerns that can affect not only a company's revenues but also their reputation and brand—bribery and corruption, data protection, performance, and broad compliance risks. For our manufacturing customers in particular, the need to manage their multiple vertical customers' regulatory requirements varies considerably and, again, enforces this notion of a value chain, versus only a supply chain.

SWITZER: Supply chains seem like perpetual motion machines—something is always changing. How do you continually monitor and adjust when there are so many moving parts?

KEVERN: Dell addresses this by having a seat at the table, conducting annual compliance risk assessments, and using data analytics technology. Having a seat at the table—whether its periodic staff meetings, quarterly business reviews, or annual leader events—is essential to remain in touch with changes in business strategy and ensure real-time discussion about potential compliance implications in light of supply chain changes. Formal annual compliance risk assessment is another means to keeping a pulse on supply chain ac-

tivity. In companies such as Dell where formal compliance risk assessment is part of the culture, business leaders expect questions such as “Are you considering outsourcing?” or “What are your financial incentive targets for resellers next year?” At Dell, it is only fitting that we leverage technology to proactively monitor our supply chain. With our automated continuous monitoring capability, we are able to identify sales activity as compared to population of sales partners cleared through due diligence; ensure third parties with a red flag are further analyzed for suitability; and ensure prospective third parties not deemed suitable for Dell business are not on-boarded or further engaged by Dell. Efficiencies achieved have allowed us to reallocate resources to identify trends, resolve exceptions, and continuously improve programs.

PATTERSON: One of the biggest drivers for technology is the threat to supply chain resilience due to the fact that the supply chain and elements of risk are constantly changing. While capturing all third-party data is important, dynamic monitoring and managing is key—this is not a static environment and no company that I know of has sufficient employees to manually monitor and manage the changes as they happen. So technology and processes that can dynamically and automatically detect and act on changes as they happen and that pro-actively adjust to changes—particularly changes in elements of risk—are essential.

WYLIE: Supply chains are ever changing and highly dependent on the flow of information up and down the value chain. Ideally, companies should follow a continuous process that begins with assessing the current state of supply chain, pinpointing critical vulnerabilities, and then creating a prioritized roadmap for improvement. Part of this assessment is capturing all third-party data in systems, which are frequently updated, and then constructing real-time visual value chain networks. By mapping value flows, geographical locations of operations, and transportation links, it is easier to see your greatest potential value losses. Equally important is the

establishment of accountability—not having a single point of accountability can lead to fragmented decision making and a tendency to optimize risk at the local or functional level, rather than for the overall supply chain. Working from this foundation, companies can implement improvements and establish processes for monitoring and managing risk over the long term.

SWITZER: Where do you suggest beginning to develop a better view into supply chains?

WYLIE: Simply put—data! Gather it and implement technology that organizes it. An extensive database of third-party information as well as specific supply chain risks, along with proven risk response strategies, helps a business quickly assess its unique situation and develop a customized set of solutions to address its most critical vulnerabilities.

KEVERN: You need to start with business leader accountability. Business leaders must clearly understand why it's important to know your third party as well as the effect on the company (and personal liability) for not doing so. Business leaders must also be committed to making a decision that may not be favorable to the local bottom line, but best for the enterprise as a whole in the long term. Business leader commitment goes hand in hand with the exercise of data discovery.

PATTERSON: All of our customers have some systems in place today that, at a minimum, give them line of sight into their critical suppliers. What they're trying to address is what they don't know below that and within those associations. And, within those associations usually lie the greatest risks. Our recommendation, therefore, is to extend the current set of information and data to address all third parties within the value chain. Most customers begin by addressing specific elements of risk or specific supply chains or criticality and progressively expand down the value chain. Think of it in terms of implementing a strategic framework and executing in a phased or sequenced approach. ■

ROUNDTABLE PARTICIPANTS



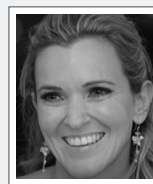
MODERATOR
Carole Switzer
President,
OCEG



Kristi Kevern,
Director Operational
Compliance,
Dell Inc.



Marie Patterson,
VP, Marketing,
Hiperos



Nicola Wylie,
Proposition Marketing
Manager – Enhanced
Due Diligence,
Thomson Reuters