SUPPLY CHAIN RISK MANAGEMENT — THE COMPLEXITIES OF MANAGING RISKS IN COMPLEX GLOBAL SUPPLY CHAINS

John. J. Brown

THOMSON REUTERS™

TABLE OF CONTENTS

Overview

In the drive to achieve business goals and ensure continued profitability, multinational organizations build relationships with customers, suppliers and partners across the globe, creating complex supply chains. Over time these "chains" more accurately resemble intricate interconnected webs. Knowing who you are dealing with in these webs becomes increasingly more difficult, yet increasingly more important.

These supply chains can be efficient at transforming materials and human capital into products and services to create revenue, profit and shareholder value. At the same time, these complex supply chains increase exposure to risks of business interruption and economic impact, less obvious risks such as corruption, theft and fraud, and to risks such as human rights abuses and environmental malpractice which can have significant impact on reputation. These risks can severely impact or even destroy an enterprise, including organizations with sophisticated and carefully maintained processes.

It is not surprising then that many successful organizations focus resources on their supply chains. Organizations are challenged, however, by the current dynamic physical, economic, political and legislative environment and the stepping up of enforcement action around the world. So how does an organization create an enterprise wide risk management framework which addresses the multitude of risks inherent in their – often complex - supply chains?

Creating and maintaining an efficient framework for supply chain risk management

Supply chains—or more accurately value chains—are a series of nodes and links. Each node represents an activity like the source of a material, conversion of materials into a product or sub-product, intermediate storage, and providing customer and consumer access to purchase products. Links represent the routes and "containers" to move materials between nodes. Each node can easily have tens if not hundreds of inputs, each of which in turn includes links to upstream nodes.

Each node and each link within a firm's supply chain poses a potential risk. It is usually not feasibleor appropriate to apply equal effort to each piece of complex value chains. How can organizations then effectively and efficiently deal with managing the risks in value chains? Mapping the flow of value through complex sets of nodes and links is an effective process to understand where effort should be placed to manage critical supply chain risks. This approach works just as well for flows of information and for providing services as it does for physical value chains.

Once the flow of value through the chain is understood, critical nodes and critical links can be identified. For instance, if a single node, say a supplier, of a particular material or service contributes to a significant portion of an organization's or product's revenue or profit, this node should be further investigated to determine risks that may exist within the operations at that node. The criticality of this node increases dramatically if there are no existing alternate suppliers of the material or service. The same can be said for links, analyzing the network for the impact of failures in any link.

In addition to analyzing risks to the value creation aspects of networks, the potential for corruption, fraud, human trafficking, etc. should be assessed. This view may require a different lens than the value creation lens, since misconduct by a relatively insignificant supplier or internal operation can still result in significant impact to an organization's reputation. Knowing who your value chain partners are, and especially how they operate becomes much more important. Due diligence processes are required for supplier selection and ongoing monitoring to detect and mitigate these types of risks.

Mapping and understanding value flows through complex value webs, and the exposure to conduct and similar risks, is unfortunately extremely difficult in practice. Many organizations find it difficult to map their value chains one level up and one level down. Going beyond this "Tier I" becomes geometrically more difficult. Yet, as we see more and more, society and governments expect organizations to know and understand their extended value chains, and as a minimum exert some level of influence over all involved parties.

How then can organizations effectively and efficiently manage risks in these complex global value webs? Perhaps the most effective approach is to create a risk management framework with supporting processes and apply these at each relevant level within the organization and its value chain. Risks are best understood by those closest to them, so it makes sense for each locally relevant entity to identify, analyze and treat risks of significance to that entity.

Creating a robust risk management framework and supporting processes is only part of the solution. Maintaining a rigorous framework of supply chain risk management is equally, if not more, important. Numerous factors can undermine the most robust of frameworks and this is largely because organizations operate in a dynamic global environment where few factors remain constant for any length of time. New suppliers are added to the chain, compliance legislation is constantly evolving, ongoing staff changesmean that processes and procedures may not always be followed with the same degree of formality and new risks are constantly emerging.

What this indicates is that the supply chain risk management framework is a dynamic model which must be regularly checked, updated and amended over time.

Out of the starting blocks, into the race

To be successful, it is important that organizations create a culture that integrates the identification, analysis and treatment of risks into business processes, including strategic planning. In the continued drive for increased efficiency, reduced costs and improved profitability, risk management all too often results in the appearance of managing risks to a level only sufficient to satisfy the apparent compliance with corporate policies. Many times this degenerates into an annual "check-the-box" mentality.

A successful risk management program supports and improves business operations. Risk management processes must be supported with easy-to-use tools. Reporting and monitoring processes are seamless, as is the aggregation of risks upwards through the enterprise and horizontally by function. This is where the right technology platform is invaluable.

Two additional characteristics must be integral to a successful risk management program. Each and every significant risk must have an identified owner and each treatment action must be assigned to an individual who is responsible for completing the action. These actions drive ownership and accountability for managing risks.

Finally, due to the dynamic nature of organizations, the environments in which they operate, and the risks they encounter, risk management must be an on-going living process. To this end it is important that each local entity have an active "risk register" to maintain an up-to-date list of significant risks and the actions agreed to mitigate those risks. To the extent possible, these same requirements should be built into agreements with all value chain partners, and likewise with these partners' partners. Difficult? Yes. Impossible? No. The right technology platform can ease the challenge and build an incredible wealth of risk intelligence across complex value chains.

Further details on risk management processes include:

- Robust processes to identify significant risks
  - » Initial selection of significant risks via a catalog or checklist
  - » Semi-structured interviews to refine significant risks
  - » Brainstorming to identify risks to strategic and business plans
  - » Mechanisms to detect emerging risks
- Intuitive, easy to apply process to analyze characteristics of significant risks
  - » Cause and consequence, including the visual bow-tie method
  - » FMEA (failure mode effect analysis)
- Identify and agree techniques to treat each significant risk
  - » Prevent the risk from occurring
  - » Ready to deploy plans to minimize the impact, or consequence, of a risk that does occur
- Construct a local risk register to document significant risks and treatment actions
  - » Reporting and monitoring programs
- Advanced techniques to maximize the value of risk management
  - » Monte Carlosimulations
  - » Scenario analyses
  - » Bayesian networks

IDENTIFYING SIGNIFICANT RISKS IN THE SUPPLY CHAIN

Many methods and techniques exist to identify risks (ISO 31010[i]). Each has unique characteristics that make it more suitable to one situation as compared to another. Risk identification techniques that are most suitable in complex global supply chains are discussed in this section.

Several characteristics of how people perceive and relate to risks should be considered. Risks that have occurred in the recent past are perceived as more relevant than those that occurred months or years ago, even though the more recent risks may actually be less likely and/or less onerous if they do occur. Another consideration is the use of group settings to identify risks, where individuals may be swayed by "group-think" or are unwilling to express true feelings depending on others in the session. Cultural differences must also be taken into consideration.

1. CHECKLIST OR CATALOGUE METHOD

Complex global supply chains are exposed to a wide range of disparate risks. This fact, and the fact that people will more easily remember recent risks, makes the use of a risk "checklist" or "catalogue" important to ensure all relevant risks are considered. Relevant risks that may exist in the global supply chain are assembled in a list organized logically along key value chain elements, such as raw inputs, ingredients or parts, manufacturing operations, logistics, utilities, human resources, quality, environmental, health and safety, legal and regulatory, etc. These checklists typically include up to several hundred potential risks. The list is updated periodically to ensure it remains relevant to the organization.

The compiled checklist is then issued to several individuals at an entity, each of whom identifies those risks that they feel are significant. Individual responses are aggregated to provide an initial prioritization of risks. Semi-structured interviews are conducted next, in individual and then group settings, to refine the identified risks into an agreed and manageable number that are considered the most significant risks for the entity.

The checklist method of risk identification is best suited when a risk management program is first implemented. It is also well-suited for periodic "recalibration" of significant risks. Since the process is simple, it can be used at intervals from quarterly to annually.

2. BRAINSTORMING METHOD

Brainstorming is an effective method for identifying risks in specific circumstances. It is generally not effective for the initial implementation of a risk management program, or for open-ended risk identification, since it can suffer from group-think.

However, brainstorming is very effective to identify risks to achieving the objectives of strategic plans, annual business plans, and specific projects.

A skilled facilitator is critical to the success of a brainstorming session. The tendency of one or a few individuals to dominate a session must be overcome, and all participants must feel free to voice their opinions and ideas.

3. EMERGING RISKS

As mentioned previously, organizations are dynamic and the environments in which they operate are dynamic. For these reasons an effective and efficient process or processes must be implemented to identify emerging risks as soon as practical. There is no one-size-fits all guidance in this area. Each organization must understand its business well enough to understand where risks may materialize and employ processes to detect them.

For example, political and economic situations in foreign locations must be monitored for developments that could affect operations. Legal, legislative and regulatory developments must be monitored for potential impact on the organization and its operations. Technological developments should be monitored to understand potential disruptive changes that can affect product offerings, manufacturing techniques, or consumer preferences. Engaging with new value chain partners and/or modifying supply chain configurations can introduce new risks which should be investigated. Finally, an organization that has a significant brand presence should monitor social media for indications that its products or operations are garnering negative reactions.

RISK ANALYSIS TECHNIQUES

As with risk identification, a number of methods exist that can be used to analyze risks (ISO 31010[i]). Each method has its strengths and is best applied taking into consideration the type of risks to be analyzed and the knowledge of those who will be involved in the analyses.

It is important to understand that as organizations move risk management out and into the organization, individuals who will complete risk analyses won't necessarily have in-depth training in techniques and methods. For this reason, variants of cause-consequence analyses are best suited, and the visual bow-tie risk analysis method can be employed with great effect. Failure mode effect analysis, or FMEA, is best suited to analyzing defined processes, but it requires a skilled facilitator as well as subject matter experts in the process being analyzed.

1. CAUSE-CONSEQUENCE INCLUDING BOW-TIE

Every risk has two characteristics: situations or events that can cause the risk to occur; and the consequences, or impact, of the risk if it does occur. The bow-tie method is a form of cause-consequence analysis and is ideally suited to guide the thinking of individuals who are not trained risk professionals. It is visual, intuitive in its application, and provides good results. The bow-tie method clearly delineates the two dimensions of risk—what can cause the risk to occur, and the consequences if it does occur—and easily relate these aspects to the likelihood and impact of the risk. The bow-tie method also clearly shows how certain actions can be taken to prevent the risk from occurring, and to create plans to mitigate the magnitude of consequence if the risk does occur.

2. FAILURE MODE EFFECT ANALYSIS (FMEA)

FMEA is an excellent tool to analyze risks within defined processes. It investigates potential failures within the process and the potential effects of those failures. The analysis results are indicative of the potential likelihood of a risk occurring and what the possible consequences might be. FMEA requires a skilled facilitator as well as subject matter experts to be effective and yield reliable results.

RISK TREATMENT ACTIONS

Risks have two dimensions: events or situations that cause the risk to occur; and the consequences if the risk does occur. Actions can be taken to prevent the risk from occurring and steps can be taken to limit the magnitude of consequences if the risk occurs.

Resources are better spent on preventing risks from occurring in the first place. For instance, if the risk of producing a sub-standard product is considered significant, implementing a strong quality assurance program and/or designing production processes to eliminate the risk is the best approach, rather than having to react by scrapping a production run or worse via a product recall. Similarly, if the risk of non-compliance with regulatory requirements is considered significant, designing and implementing a program to ensure all relevant regulations are identified and processes created to meet the requirements is the preferred approach. In the case of third-party providers, developing standards and auditing against those standards is a typical approach to preventing risks such as human rights abuses and environmental damage.

As much as we would like, it is often not possible or economically feasible to prevent all risks from occurring. Therefore, developing pre-thought out plans to react to a risk event's occurrence is a prudent course of action to mitigate the magnitude of negative consequences. For instance, if the loss of a critical manufacturing site or supplier would cause significant damage to value creation, creating a backup site or multiple suppliers may be warranted.

Supply chains — or more appropriately value chains — present a bewildering array of choices in a dynamic and ever-changing environment. For these reasons, a detailed discussion of risk treatment actions is not included in this paper. The key is to understand the characteristics of significant risks and take appropriate measures to first prevent the risk from occurring, and second reduce the magnitude of consequence if the risk does occur.

CREATE A LOCAL RISK REGISTER

After the initial set of significant risks at an entity has been agreed and analyzed, and risk treatment actions determined, this information must be captured in a local risk register unique to the local entity. The risk register contains the relevant characteristics of each risk, including causes and consequences as well as actions to mitigate the risk. Each risk has an assigned owner and each treatment action is assigned to an individual accountable for completing the action.

Since risks are dynamic, the risk register is updated on a frequent and regular basis. As new risks are identified and analyzed, they are added to the risk register. When risks become less significant they can be removed from the risk register. Status of risk treatment actions are tracked via the risk register. In essence, the risk register is a living playbook of risks.

Local risk registers form the basis to provide an enterprise-wide view of risks. For example, consider an organization structure with a corporate level, and three groups, each with three business units. Group one can have an aggregated view of risks relevant to the business units within the group, which provides the group with knowledge to better understand risks relevant to its part of the overall entity. Similarly, Corporate can have an aggregated view of risks relevant to all groups, and thus better understand enterprise-wide risks. If risks are categorized by function as well, it is possible to obtain a functional view of risks across the organization, which can guide the development of appropriate policies, procedures and tools.

Value chain partners can also create a risk register to include risks relevant to the relationship and contractual obligations with your organization. Obviously this requires the partner to implement a risk management program and provide to your organization information on relevant risks. A certain level of trust is required for this to be effective, and a robust technology platform greatly simplifies the process. The depth of information, or intelligence, obtained about risks in the extended value chain, and knowing who your partners are, often outweighs the effort required to implement such an arrangement.

REPORTING AND MONITORING PROGRAMS

Reporting and monitoring of risks within an organization is imperative to the success and value of any risk management program. Incorporating a review of risks—and actions being taken to mitigate those risks—within existing business meetings integrates risk management into business operations.

Typically the simpler and more visual the reports, the better they are understood and accepted. Each organization has its own unique approach to reporting information at various levels of the organization, and it is important to provide risk information in a similar vein.

ADVANCED TECHNIQUES

Many advanced techniques exist to more fully understand and analyze risks in complex systems. Three will be briefly mentioned. Although these methods can provide increased understanding of risks, they are dependent on accurate input data used to characterize the systems. For many risks it is difficult to accurately characterize probability curves, which can render an otherwise elegant analysis less useful. Likewise, characterizing the interaction among risk events can be fraught with error.

1. MONTE CARLO SIMULATION

Monte Carlo simulation treats inputs (e.g. likelihood and consequence) as random inputs defined by probability distributions. Each run randomly selects a value for likelihood and for magnitude of consequence and combines them into a risk level. By running thousands of calculations, a risk curve is created. This technique is useful in understanding the effect of uncertainty in risks, but it is dependent on the accuracy of the probability distributions relative to the risk being analyzed.

2. SCENARIO ANALYSES

Scenario analysis is a technique useful to understand possible future states based on assumptions that can affect those states. This technique is useful in analyzing various strategies that an organization may take. Variations in assumptions — such as inflation, regulatory developments, or consumer preferences — are considered along with their effects on business parameters. Scenarios considering differing levels of risks can help determine the most appropriate actions for the business. The success of scenario analyses depends on a skilled facilitator, participants' understanding of the risks relative to the business, and group dynamics.

3. BAYESIAN NETWORKS

Bayesian networks is useful to understand interactions among elements in complex systems. Risks seldom exist in isolation and Bayes networks is a technique useful to understand interaction among risks. For example, it facilitates modeling the probability of risk Z happening given risk A and risk B. Since global supply chains are intricate networks this may be a useful technique to employ, although the effort to construct a Bayes network may outweigh the benefits.

Special Considerations for Suppliers, Vendors and Partners

The drive to increase profitability and streamline operations turns many organizations to increase outsourcing of non-core activities. While these decisions can and do result in economic benefits, attention must be given to the potential increased costs to ensure these business partners adhere to legal requirements as well as implied standards of conduct.

Why? Because in today's business environment organizations are held responsible for the actions of suppliers, vendors and partners in addition to theirown internal activities. Therefore it is critical that a robust risk management program include due diligence in the selection of business partners as well as on-going monitoring activities.

As discussed earlier, requiring value chain partners to implement a risk management program and share information about risks relevant to your organization can provide invaluable knowledge about your extended value chains.

Integrating Risk Management into Business Operations

Businesses are dynamic, and so are the risks that affect organizations. As alluded to earlier, sustaining a robust risk management framework and program is as important, if not more so, than implementing one. Three supporting risk management processes can help ensure a sustainable program: periodic risk reviews; identifying risks to achieving strategic and annual business plan objectives; and identifying and considering new risks. Timely risk communication processes must also be an integral part of a sustainable risk management program.

1. PERIODIC RISK REVIEWS

Adding a review of risks that are included in the local risk register as an agenda item to an existing business meeting embeds risk management into business operations. The frequency of risk review is dependent on the business cycle and dynamics. Generally, between once per month and once per quarter is sufficient. The review should include discussing changes in the level of likelihood and consequence, status of actions taken to treat the risks, eliminating risks that are no longer significant, and adding new risks.

2. RISKS TO STRATEGIC AND ANNUAL BUSINESS PLAN OBJECTIVES

Existing risks (in the local risk register) should be considered when creating strategic and annual business plans. When the plans are nearing completion, risks to achieving plan objectives should be identified and, if significant, these risks should be included in the local risk register for active management.

3. IDENTIFYING EMERGING AND DEVELOPING RISKS

The organization should have processes to identify new risks that are created by changes in socio-politico situations, social media activity, results of audits, developing or changing regulations, and changing economic climates, for example. We also recommend using the risk checklist/survey on an annual basis to ensure all significant risks are captured and considered.

Conclusion

It has been said that the elevation of risk professionals to the 'C' suite – in other words their relatively recent placement on a par with Chief Executive Officers, Chief Financial Officers and Chief Operating Officers – is proof of the invaluable contribution which risk officers are making to global business.The complexity and interconnected nature of supply chains increases the importance of—and the challenges with—establishing a robust, effective and sustainable supply chain risk management program.

Customers, consumers and governments hold companies accountable not only for their own actions, but the actions of suppliers, vendors and business partners as well. Understanding, and effectively managing, internal and external supply chain risks is critical to the success and profitability of today's organizations.

REFERENCES

Background reading:
http://www.weforum.org/issues/supply-chain-risk

ISO 31000:2009 Risk management — Principles and guidelines

[i] ISO 31010:2009 Risk management — Risk assessment techniques

About the Author

JOHN J. BROWN

John J. Brown, former Managing Principal in Thomson Reuters Risk Segment, is a registered professional engineer, Associate in Risk Management-ERM (ARM-E) and Certified Protection Professional (CPP). With nearly two decades of deep governance, risk and compliance (GRC) experience, John brings expertise in enterprise and operational risk management in large global companies. He also has hands-on experience in compliance and governance within the food & beverage and electronics industries, including policy creation and auditing.

Prior to joining Thomson Reuters, John was Director, Risk Management, Supply Chain & Technical at The Coca-Cola Company, where he created an ISO 31000-based risk management program and processes across the company's global value chain. Previously at H.J. Heinz John created systems and processes for operational risk management across the company's global operations. At both companies John served as a risk management thought leader and subject matter expert, developing purpose-specific risk management solutions. John is past president of the Supply Chain Risk Leadership Council, a group of industry risk management professionals with the aim to develop best practices and standards in supply chain risk management.