GLOBAL
Supply Chain Resiliency
COUNCIL



ULTIMATE GUIDE TO SUPPLY CHAIN RESILIENCY PROGRAM SUCCESS

Version 1.0: March 26 2015

resilinc
POWERING THE RESILIENT SUPPLY CHAIN

© Resilinc, Inc. All Rights Reserved.

Table of Contents

Executive Overview....2
Introduction....3
1. Plan Phase....4
1.1. Business Case....5
1.1.1. Statement of Purpose and Goals....5
1.1.2. Business Strategy Alignment....7
1.1.3. Overcoming Objections....7
1.1.4. Return on Investment (ROI) Analysis....9
1.2. Program Scope....13
1.2.1. Business Context....13
1.2.2. Program Scope Dimensions....14
1.3. Core Program Services....16
1.4. Core Service Metrics....18
1.5. Technology Plan....19
1.6. Program Office Team, Governance and Stakeholders....20
1.7. Timeline and Key Milestones....24
1.8. Program Funding....26
1.9. Charter....26
2. Implement Phase....27
2.1. People....27
2.2. Process....27
2.2.1. Risk Intelligence Service....29
2.2.1.1. Supply Chain Network Mapping....29
2.2.1.2. Supplier/Node Data Collection....29
2.2.2. Risk Analysis Service....31
2.2.2.1. Risk Identification....32
2.2.2.2. Risk Criteria....33
2.2.2.3. Risk Appetite/Tolerance....35
2.2.2.4. Risk scoring....36
2.2.3. Risk Treatment and Response....39
2.2.3.1. Risk Mitigation....40
2.2.3.2. Risk Crises Preparation....42
2.2.3.3. Risk Recovery Preparation....46
2.2.4. Risk Monitoring & Response....47
2.2.4.1. Event Monitoring....47
2.2.4.2. Supplier Monitoring....48
2.2.4.3. Risk Tactical Response....50
2.3. Technology....52
3. Institutionalization....56
3.1. Program Monitoring and Management....56
3.2. Working with Governance and Senior Leadership....57
3.3. Team motivation and incentives....58
3.4. Operationalizing Supply Chain Resiliency and Risk Management....58
3.5. Positioning the Program for Future Success....61
Conclusion....63
Acknowledgements....64
Disclaimer....65

Executive Overview

The goal of this white paper is to provide supply chain risk management practitioners with concrete suggestions and guidance on how to create, roll-out, and institutionalize a global supply chain resiliency program (SCRP). Supply chain resiliency starts with end-to-end supply chain visibility and includes comprehensive strategies to sense and manage supply chain risks proactively and in a highly responsive manner.

Further, SCRPs are strategic programs, not operational programs. As such, the goal is to identify strategic and high business-impact risks for mitigation. Risk treatment or the execution of risk remediation measures is, at least in part, if not in whole, the purview of operational business practices and systems. As a result, the role of SCRP programs and systems is primarily to recommend, prioritize, and track mitigations that are, in turn, executed by operational teams.

The premise of this guide is that there is an unserved need for information on the topic of building and managing a SCRP that adequately addresses the crucial initial phase of building the business case, establishing strategic alignment, and securing executive sponsorship. While best practices in this area have perhaps been documented and shared, they are not integrated into a broader program deployment and operational plan.

This guide also attempts to untangle the confusing array of processes and labels for those processes, put forward (e.g. risk assessment, risk analysis, risk evaluation), as well as the loosely associated best practices. This guide aims to refresh and organize program implementation and maturation best practices into a single comprehensive and easier to navigate reference and starting point for building a world-class supply chain resiliency program.

Further, this guide is organized as a simple roadmap and not a more elaborate maturity model. Key insights from leading maturity models are embedded in the roadmap. While the guidance and insights are intended to apply broadly across vertical industries, individual enterprises should evaluate the relevance of the topics and recommendations based on their unique business context and embrace suggested best practices based on the maturity of its risk management and resilience people, processes and technology.

Finally, this is version 1.0 of what is intended to be a living document. The goal is to improve this document over time based feedback from the Global Supply Chain Resiliency Council membership community and other industry practitioners and research scholars.

According to a recent study, supply chain risk management has emerged as the second largest challenge for operations executives after supply chain visibility – placing even higher than increasing customer demands and higher costs.

Introduction

The Supply Chain Resilience Program (SCRP) roadmap described here consists of three primary phases: Plan, Implement and Institutionalize. Each phase is broken down into a number of sequential elements. This document walks through each step individually and elaborates as necessary on the various concepts and recommendations presented.

Before proceeding, it will be instructive to define two key terms:

Supply chain risk. The likelihood and consequence of events, at any point in the end-to-end supply chain, to disrupt the normal flow of supplies.

Supply chain resilience. The capability of a supply chain network and individual suppliers to recover quickly and cost-effectively from an event and with minimal or no impact to the normal flow of supplies.

1. Plan Phase

The plan phase is organized around asking and answering why, what, how, who and when with respect to supply chain resiliency programs (SCRPs). The answers to these questions form the core information that flows into the SCRP charter. The initial plan phase should not be exited until the SCRP charter is completed and buy-in is confirmed from key stakeholders and customers identified in the planning process. The charter should take the form of a one- or two-page summary document that addresses most or all of these key program questions.

TABLE 1. THE CORE INFORMATION NEEDED FOR THE SCRP CHARTER

	KEY PLAN COMPONENTS	KEY QUESTIONS ANSWERED
WHY?	Business case	Why form a SCRP (fundamental purpose and goals)? What strategic business goals are aligned with the supply chain resiliency program goals? What objections need to be overcome? What is the expected ROI?
WHAT?	Program scope	What is the scope of the SCRP and the funding requirements? What core services will the SCRP provide and what is out of bounds? What will success look like and how will it be measured and communicated?
HOW?	Business processes & technology	How will services be defined and delivered? What role will automation play?
WHO?	Governance, customers/ stakeholders, SCRP team structure	Who is the executive sponsor/champion? To whom does the SCRP report? Who are the SCRP's customers and stakeholders? Who comprises the dedicated SCRP team?
WHEN?	Timeline/ milestones	When will the SCRP be in business and when will the core services come online? What are the key program milestones and target timeframes?

1.1. Business Case

A successful business case includes (1) a clear statement of purpose and business goals, (2) an understanding and response to anticipated program objections, (3) a clear alignment with the business strategy, and (4) an ROI analysis.

1.1.1. Statement of Purpose and Goals

A simple statement of purpose and goals should serve as a guide for the SCRP team and as a core communications platform to business leadership and supply chain stakeholders. Potential goals range from strategic to the more tactical.

Critical Success Factors and Best Practices:

- Identify several strategic program objectives and supporting tactics.
- Provide the strategic context and influences by describing the key business drivers. For example:
  - Supply chain networks are larger, leaner, more global, more interdependent, more complex, less transparent, and changing more frequently.
  - Customer expectations continue to grow.
  - Commodity costs are increasing.
  - Logistics capacity remains constrained.
  - Natural disasters impacting globalized supply bases are on the rise as a result of global warming.
  - Brand risks are increasing as a result of supplier compliance, corporate social responsibility, and security practices.
  - New product introductions have been more frequent
  - Products and services have become less standard
- Use the table below to brainstorm strategic objectives and tactics.
- Aim for strategic and tactical goals that are ambitious, yet achievable.
- Ensure program strategies drive or support C-level corporate strategies.
- Consider tactics that may be viewed as transformative (i.e. fundamentally change the way supply chain risk management processes are performed today).
- Package strategic objectives and tactics into a simple statement of purpose and goals that can be easily shared and understood.
- Position SCRP purpose and goals as complementary and accretive to existing enterprise risk programs.

TABLE 2. POTENTIAL SCRP PROGRAM STRATEGIC AND TACTICAL OBJECTIVES

Sample Strategic Objectives	Sample Tactical Objectives
Achieve competitive advantage (turn business disruption threats into opportunities)	Decrease supply chain related insurance premiums
Protect brand value and customer satisfaction (based on customer service level data)	Facilitate supplier collaboration and information sharing
De-risk revenue and time to market goals	Avoid supply chain costs (e.g. component buy-aheads, emergency second sourcing, expedited freight, etc.)
Decrease operational costs	Reduce inventory
Protect shareholder value	Improve supplier quality
Ensure continuity of supply through a controlled, predictable response	Improve lead times and variability
Manage regulatory/compliance exposures	Improve delivery/order fulfillment performance (on-time, variability)
	Reduce number of supply crises impacting critical products or parts
	Reduce incident response times and time-to-recover for the highest priority supply chain activities, products and services
	Improve supply chain asset utilization and inventory turns

1.1.2. Business Strategy Alignment

The program should be directly linked to core C-level revenue, customer satisfaction, and cost/operational metrics.

Critical Success Factors and Best Practices:

- Ensure executives understand the direct linkage between revenue forecasts, time-to-market assumptions, and supply chain disruption risks.
- Ensure executives understand the direct link between customer satisfaction, brand value and supply chain disruption and delivery risks.
- Ensure executives understand the empirical evidence/correlation between material supply chain events and shareholder value.
- Ensure executives and line of business stakeholders understand any connections to existing supported supply chain objectives in areas such as quality, environmental/sustainability, and occupational health and safety management.
- Set proper expectations with respect to what is possible given the broader organization's strategic value drivers and their key supply chain value drivers. For example, of companies with more mature resiliency processes in place, those that focus more on flexibility and customer service levels demonstrate higher performance resilience compared to companies whose strategies emphasize cost and efficiency. This is counter-intuitive when you consider that low variability is one of the key drivers of an efficient operating strategy. [1]

1.1.3. Overcoming Objections

Resistance to supporting and investing in SCRPs is in part the result of professional incentives, psychology, misperceptions about costs, and a lack of awareness and education. Understanding the role that each of these factors may play and being prepared to neutralize the resulting objections is key. In general, typical objections can be categorized into six primary categories described next.

Incentives and human nature. At the core of the incentive issue is that few executives are compensated or incentivized in their day-to-day job to rigorously manage risks. What has been described as risk apathy is driven by supply chain executives who often find themselves at the center of the daily storm, striving to balance very demanding operational objectives while satisfying customers, cutting costs, and helping grow revenue. They must deliver results today while working on capabilities that will make companies competitive in the future.[2] From a psychology perspective, it is easier to focus on the burning short-term issues that are here and now than worry about the next black swan event. As a result, it is easier to put off investments in risk management.

Dependence on supplier collaboration. A typical objection to investing in a supply chain resilience program is the dependence on supplier transparency and collaboration. Many organizations see resilience programs (especially those whose value proposition depends on n-tier supplier visibility) as a non-starter since historically suppliers have

been reticent to share information that they fear may be used against them, for example, in financial negotiations. A lack of data standards and varying supplier IT maturity levels can further hinder an effective data exchange.

Perceived cost of visibility. Another common point of resistance is cost, especially the perceived cost to achieve end-to-end supply chain visibility. It can seem daunting to ponder the cost of supporting an internal team to reach out to potentially thousands of suppliers and collect and maintain data at the necessary level of granularity, integrity, and accuracy over an unbounded period of time.

Conflicting objectives. Many supply chain risk management tools and remedies seem at odds with popular supply chain cost efficiency strategies such as lean inventory management and other measures to reduce cost while remaining innovative. As a result, various stakeholders may hesitate to get behind a program they view as increasing costs by supporting measures such as building buffer inventory and engaging alternate/redundant suppliers. Moreover, the relentless focus on cost reduction as a pervasive business objective and metric causes the need to focus on risk-reducing objectives – such as quality, on-time delivery, responsiveness, diversity, and supplier viability – to be overlooked.

Outmoded thinking and assumptions. There are several biases, attitudes, and dangerous assumptions underlying common supply chain practices that can devalue or not properly credit risk and resiliency measures. They include faith that "operations will always save the day with another extraordinary diving catch" and that the commodities team can "gut" their way through a problem. Another dubious refrain is "we got lucky that time" rather than recognizing that, more often than not, it was not pure luck that an impact was not felt, but the actions that somebody took to select a supplier located on higher ground or to find an alternate source. There is also an assumption that risks are typically isolated and not interlinked. There may be little appreciation for how a SCRP can ascertain how vulnerabilities that pop up in one area may be symptoms of wider and more systemic issues.

Further, some supply chain stakeholders are under the impression that they can rely on their suppliers to address risk issues, financial, CSR/ethics, etc. in the sub-tiers. According to ChainLink Research, however, audit and regulatory visibility falls off after tier 2. There may be little awareness of the need to take an end-to-end approach which is a fundamental assumption of most SCRPs.

Finally, there is a major pre-occupation with the so-called "black swan" events (i.e. infrequent disaster scenarios). This has two potential negative impacts to the perceived need to invest in a SCRP. First, many believe these "acts of gods" by definition can't be predicted and planned for, so preparation and mitigation is futile. Rather, these are frequently scenarios that catch supply chain professionals uninformed/unaware. There are in fact early warnings and information foreshadowing most events, yet most organizations have no access or visibility to that data. Second, these events distract from the focus that a SCRP applies to the smaller, but almost daily, supply events that in aggregate have a larger business impact.

Resiliency measures such as improving visibility to supplier lead-times, time-to-recovery, and alternative sources of capacity may drive decisions to reduce rather than buffer inventory.

Difficulty in valuing risk management. A companies' inability to calculate and collectively agree on how to value risk due to a supply chain disruption can obstruct making progress in risk management efforts.[3]

Critical Success Factors and Best Practices:

- Educate leadership on how SCRPs align with strategic objectives and how a failure to act can derail the achievement of strategic goals.
- Provide empirical evidence of the probability of a significant supply chain disruption event and the short and long-term business and financial consequences. [Recommended resource: Georgia Tech, Kevin Hendricks & Vinod Singhal: An Empirical Analysis of the Effect of Supply Chain Disruptions on Long-run Stock Price Performance and Equity Risk of the Firm, 2005]
- Speak the language of business value and prepare an ROI analysis (see section 1.1.4 below)
- Provide a dispassionate analysis of alternative solutions or taking a "do nothing" approach to the supply chain resilience and risk management challenges and the consequences of not pursuing a SCRP.
- Develop and communicate strategies and plans to mitigate the risk of suppliers not collaborating in the development of your multi-enterprise resiliency program such as:
  - Education, coaching, and help building broad supply chain capabilities that improve the overall business.
  - Incentives, rewards, recognition/preferred status.
  - Help finding other customers to improve financial stability.
  - Productivity and ease of secure "publish once, share multiple times" cloud data sharing model.
- Develop a preliminary program cost estimate leveraging low-cost service providers in areas like supplier on-boarding.
- Address "conflicting objectives" head on by educating stakeholders on the need to balance what Cisco characterizes as the "resiliency challenge" – balancing speed and flexibility, and how to be innovative while being resilient.
- Converge on a risk value standard that is based on revenue impact and avoid arguments about the probability of disastrous events occurring or how to value things like brand impact. Provide best- and worst-case revenue impact scenario and mitigation cost estimates that can be compared against established risk tolerances so that decisions can be made using a consistent process.

1.1.4. Return on Investment (ROI) Analysis

Executive decision makers frequently require an ROI analysis before approving a significant investment. It is important to understand the practical goals and limitations of any ROI analysis.

ROI analyses are useful in the process of persuading the approving powers by providing a more structured and monetization-driven argument. However, it may play a limited role in the overall decision which can ultimately place more weight on cultural factors like "ability to execute" and considerations and benefits which are difficult to measure, like alignment with strategic objectives.

Another limitation is that the results are challenging to verify even after the return (positive or negative) has been realized. Executives that request an ROI analysis recognize this but still see value in imposing the rigor required by this activity as an important piece of the business case puzzle.

Finally, it's important that decision makers not lose sight of the strategic "return" on a SCRP investment which is difficult to calculate. This includes the value of enhanced customer satisfaction, brand value, and competitive advantage associated with optimized product availability and business continuity.

Generic formula: [(Incremental revenue + cost savings) – Investment] / Investment

Assumptions and Best Practices:

- ROI should be calculated over a three-year period to provide ample time to ramp up the program, people, processes and systems.
- The recommended approach assumes that some risk mitigation and resiliency practices and investments are in place previous to the SCRP launch. As a result, only the net or incremental revenue or cost impact should be included in the ROI calculation.
- "Be creative and look holistically when driving initiatives and evaluating ROI. Collaborate with internal departments to understand how the data you're collecting and the initiatives you are driving can help to advance their interests in parallel. For example, sustainability teams often have similar interests in emergency preparedness practices and the labor standards they are likely driving with your suppliers can reduce the risk of disruption rom strike or riot."

  – Matt Mills, Principal Program Manager, EMC

Resilinc's experience with clients combined with market research shows that a SCRP program can save up to $15 million for every $1 billion in annual sales.

TABLE 3: ROI FRAMEWORK AND WORKSHEET

ROI COMPONENT	SUB-COMPONENTS AND NOTES
Incremental Revenue	
Expected revenue value of proactive risk mitigations	This is a significant estimation/analysis in and of itself. It can be derived using historical annual information on the average number and average revenue impact* of previous events and estimating what percentage of that impact would likely have been avoided. This will require making several assumptions; it is best to provide best and worst case scenarios. Including supplier capacity risks and management as part of your SCRP purview can augment expected revenue by being better prepared for "positive risks" such as sudden demand surges.
Expected revenue value of improved reactive event response	This is the revenue loss avoided by responding more rapidly to disruption events and minimizing time-to-recovery. This can be estimated by gathering historical information on the number of events responded to of varying impact/consequence profiles (e.g. severity, products affected, etc.) and the time it took to sense, respond and recover. The next step is to create a model portfolio of projected events and event profiles for a given year and estimate the number and value of shipping days saved by having an improved response capability.
Cost Savings	
Operational costs	These are incremental costs avoidance opportunities that may result when SCRPs are deployed and bring to bear the benefits of proactive planning and analytics: > CBI insurance premium and improved coverage savings > Emergency second sourcing costs > Expedited freight costs > Savings from advanced (sub-tier) sourcing and preferential pricing arrangements > Contingent/temporary labor costs avoided > Inventory holding costs (e.g. idle inventory resulting from a disruption) > Switching costs to alternative suppliers > Component forward buying and hedging > Reduction in recall/settlement payments

Productivity	These are incremental cost/time savings associated with SCRP staff or stakeholders performing and executing a variety of risk management tasks and processes in a less manual and more automated manner. It is assumed that personnel can be refocused to perform other or higher-value tasks as a result of productivity improvements. To estimate annual savings it is necessary to determine the number of individuals currently performing these activities and survey them on the hours spent per week/year. It is then a straightforward calculation of aggregate cost by multiplying hours spent by the fully-loaded full-time-equivalent (FTE) cost of an employee per week/year. > Supplier information data collection and management > Supply network mapping and updating > Information searching (individuals spend up to 20% of their time searching for information when there is no single information repository) > Ad hoc information requests about suppliers from internal stakeholders (e.g. commodity manager not disrupted and has 50% more time for higher value tasks) > Information reporting (individuals can spend 20-40% of their time generating and formatting manual reports; centralized dashboards and reporting systems can eliminate this time) > Mitigation planning and analytics/scoring > Budget/resource prioritization > Event monitoring > Event impact analysis
Investment	
Headcount	This is the incremental program headcount including dedicated and part-time staff as well as allocated resource costs.
Program	This includes any program budget for marketing/communications, meetings/events, travel, or other ancillary costs associated with the program.
IT	This covers the cost for any: > Annual cloud system subscription fees > Annualized/depreciated perpetual software license fees and hardware > IT consulting services > Maintenance and support > User/admin training

* Revenue impact is calculated by determining the number of days of forecasted product shipment (# of products multiplied by dollar value) that is disrupted by a supply chain event.

1.2. Program Scope

By detailing what is part of the program and what is not, it will be possible to better put into context program goals and objectives (described above) and set more clear and realistic expectations for program results. The first step in determining scope, however, is to understand the business context or environment in which the SCRP will operate.

1.2.1. Business Context

Understanding the basic internal and external business conditions and drivers in which the program operates is an important part of the planning process since it serves as an ability-to-execute reality check. A more detailed analysis will be required during the implementation phase and on-going monitoring will be required during the institutionalization phase to ensure that the underlying assumptions about the business on which the program has been built have not shifted over time.

Note: *As indicated in the executive overview, a premise of this guide is that a SCRP is a strategic planning and not operational execution program. SCRP processes will therefore interface/integrate with operational processes rather than subsume them.*

Critical Success Factors and Best Practices[4]

- Identify the internal environmental factors that can impact program scope such as:
  - Business objectives, value drivers, and strategy initiatives (see also 1.1.2 Business Strategy Alignment).
  - Organizational model (centralized vs distributed governance, decision-making, accountability, funding)
  - Resources and capabilities
  - Culture
  - IT
  - Maturity level of supply chain and dependent business processes
  - Other related policies, communication and consultation protocols
- Identify external environmental factors that can impact program scope such as:
  - Supply chain interdependencies
  - Legal, regulatory and contractual obligations
  - Economic, social, political/government and cultural considerations
  - Geographic and community factors
  - Financial and competitive environments
  - Communication and logistic factors
  - Market, brand/reputation and media relations

1.2.2. Program Scope Dimensions

There are several dimensions which can be used to determine and describe the appropriate program scope. One, or more typically, a combination of dimensions described below should be adopted for communication and expectation-setting purposes depending the organization's unique risk profile.

- **Risk type identification approach**. A SCRP may be defined around a selection of target risks that need to be managed. One of the many published supply chain list catalogs or supply chain risk taxonomies can be used as a starting point. ChainLink Research, for example, provides a taxonomy which breaks risks into 5 major categories: financial/market, operational, geographic, corporate social responsibility, and regulatory economic [See "Supply Chain Risk Solutions: A Market Overview," 2013].
  - Note: Risk type identification is a necessary exercise regardless of whether or not it is used to describe SCRP scope. For the purpose of describing program scope, a risk type driven program minimally identifies a set of relevant and vetted risks based on strategic/executive-level concerns, experience and consequences with previous supply chain disruptions or incidents, and/or high-level analysis of future vulnerabilities. It is a pre-requisite for the subsequent and more precise risk scoring phase (see section 2.3.2.4) which identifies and quantifies the likelihood, frequency, and consequences of specific risk vulnerabilities at a supplier, site, product, or part level.
- **Supply and demand chain approach**. A SCRP can encompass some or all phases in a supply and demand chain from upstream processes such as product design and development, to sourcing and manufacturing, to downstream delivery logistics and customer support. This life cycle is described as Source-Make-Deliver-Return (SCOR Model) and there is a unique set of risks that can be mapped to each of these phases. Many organizations take this approach and start with a program scope that focuses primarily on the "source risks" and within that phase focus only on upstream Tier 1 suppliers, at least initially, before expanding the scope end-to-end. Within Tier 1 organizations, the scope may be further narrowed to focus on a specific segment or number of named "highest risk" suppliers.
- **Internal versus external risk approach**. An SCRP can focus on internal risks to supply chain (e.g., supply quality, supplier reliability, production/equipment reliability, demand forecasting) and external risks such as natural disasters, geo-political events, labor strikes and factory fires.
- **Risks to tangible versus intangible assets approach**. An SCRP program can focus primarily on managing risks to tangible assets such as human, physical or financial resources. Alternatively, the focus may be more on intangible resources such as brand, reputation, IP or competitive positioning.[5]
- **Solution/Tool-driven approach**. While technology decisions should normally conform to people and process needs rather than the reverse, some organizations will adapt a technology platform and its inherent risk management focus which, for all intents and purposes, defines the program scope. They then configure the

solution to the extent possible and extend the platform working with the vendor as a strategic partner to influence the product roadmap.

- In an emerging early-stage and fragmented market for solutions, this approach can make a lot of sense. By definition it ensures that there are tools that align with your in-scope program processes, rather than risking having to cobble together a set of point solutions. Also, the emerging vendors are eager to work closely with large enterprises to validate their solution and build reference accounts.
- ChainLink Research, for example, provides a supply chain risk solution and services taxonomy which breaks solutions into four intersecting major categories: supply chain mapping and monitoring, supplier risk and compliance, traceability/chain-of-custody, and risk and business continuity consultants [See "Supply Chain Risk Solutions: A Market Overview," 2013]. Gartner identifies four primary enterprise system categories: sourcing due diligence, regulation-specific compliance, ERP/quality software modules, and cloud systems (see 2.4).

> **Supply Chain Initiative-Driven Approach**. This approach focuses on pursuing various supplier information base initiatives that are either directly or indirectly associated with supply chain risks. These include disruption risk, business continuity/recovery risk, capacity risk, compliance risk (e.g. conflict minerals), corporate social responsibility (brand risk) and security risk. To the extent that solution/tool vendors take the approach of building solution modules for each supply chain initiative, this approach may be virtually synonymous with the solution/tool vendor approach described above.

> **Supply Risk Management Approach**. An SCRP may focus on (1) proactive risk management (efforts to decrease the likelihood and consequences of a supply chain risk event), (2) incident management (efforts to minimize the negative consequences of an event after it has occurred) and/or (3) risk avoidance/elimination/transfer management. Increasing second sourcing is an example of how risk can be reduced or eliminated. Increasing inventory is a tactic for mitigating supply risk, while insurance can be used to transfer risk to a third party.[6]

> **Other Approaches**. Other potential scope dimensions include "supply chain versus services chain" This guide focuses on supply chains, but its worthwhile understanding what processes, practices, concepts and ideas can be applied or cross-pollinated with service chain resiliency efforts.

Critical Success Factors and Best Practices

> The right answer typically blends elements of more than one approach. For example, a typical SCRP scope may start with a focus on select supply chain initiatives supported by a strategic technology or consulting services provider. The first phase may further focus only on select risk categories for tier 1 suppliers and then expand the types of risks and the number of supply chain tiers under management.

> When taking the Supply Chain Initiative-driven Approach, core (disruption) risk management should always be complemented with business continuity planning (BCP) and capacity management solutions in order to provide a more complete resilience program. For example, business continuity measures should be in place to minimize supplier recovery time in the event of a disruption. Proactive collaboration with suppliers may be invoked in the event that a supplier has constrained capacity in a short-to-medium term planning window.

1.3. Core Program Services

Now that you defined the core SCRP mission/purpose and program scope, the next step is to identify the key services that the SCRP proposes to offer in support of its business goals. The table below describes various potential SCRP services offerings. Some organizations may focus on a few of these areas, while others take on all of these areas over time.

TABLE 4. POTENTIAL SCRP SERVICE OFFERINGS

SERVICE AREAS	SERVICE COMPONENT
Risk intelligence	Services to map supply chain network end-to-end including individual supplier manufacturing footprints
	Services to achieve supplier visibility by collecting, validating and maintaining supplier data via surveys and/or other supplier information sharing and collaboration tools
Risk analysis	Services to identify and address current supply network vulnerabilities (e.g. single source and/or high-revenue impact suppliers and parts)
	Services to assess supplier preparedness and time-to-recovery (business continuity plans)
	Services to assess supplier capacity to handle demand surges.
	Services to develop well-rounded supplier "risk scores" taking into account financial, location, recovery risks combined with sourcing and operational risk scores
	Services to develop a prioritized plan to remediate individual supplier and product/part issues (e.g. second sourcing, strategic inventory buffers, capacity reservations)
	Services to manage security, brand risk (CSR) or other supply chain resilience dimensions
Risk treatment	Risk mitigation planning services to recommend mediation options and track status/progress to completion
	Risk crises preparation planning services
	Risk recovery preparation and continuity planning services

"Balance mitigating specific risks with building broad capabilities. Focusing on the management systems and BCI processes of your suppliers can often drive more "bang for your buck" than mitigating specific areas of risk."

Matt Mills
Principal
Program Manager
EMC

Risk monitoring and response	Services to monitor, sense and generate alerts for potential supply chain disruption events globally 24X7 Services to monitor/audit suppliers and change notifications Services to assess and organize a cross-functional rapid response to supply chain events and incidents mobilizing pre-determined playbooks, war room capabilities and visualization tools

ISO 31000 provides a framework of risk management processes that can also be used to create your own services model.

Critical Success Factors and Best Practices:

- In order to achieve maximum effectiveness, to the extent possible, these processes or services should be integrated into existing business planning and management processes.
- Both the business context (culture, strategic objectives, supply chain needs and characteristics) and the most significant risks are constantly evolving making it essential to continually re-align the program process/services and metrics to ensure relevance and effectiveness. Recognize that the current program definition and plan is only valid in the context of the current operating environment. As a result, sustainable relevance will depend on the ability to manage change and pivot with agility.

1.4. Core Service Metrics

Metrics for managing the performance of each service offering need to be defined. More "outside-in" business driven SCRPs may focus on contribution to external business metrics such as return on investment (ROI), time to market (TTM), and customer satisfaction, while more traditional SCRPs typically define metrics for various service offerings (see Table 5 below).

TABLE 5. DEFINING METRICS FOR EACH SERVICE OFFERING

POTENTIAL SERVICE	EXAMPLE METRICS/ SUCCESS CRITERIA
Risk intelligence	Number of suppliers/tiers mapped
	Number of suppliers and supplier sites fully on-boarded
Risk analysis	Number of vulnerabilities identified
	Expected aggregate revenue impact of vulnerabilities identified
	Expected aggregate revenue impact of vulnerabilities mitigated proactively
	Expected aggregate cost impact of vulnerabilities mitigated proactively (cost avoidance)
	Supplier resiliency scores/index based on financial health, BCP compliance, etc.
	Manufacturing resiliency scores/index based on time to recovery (TTR), dual site or qualified alternates
	Product resiliency scores/index based on supplier/ component risk, etc.
	Cost savings from reduced contingent business interruption (CBI) insurance premiums
Risk treatment	Number of mitigations launched and completed
	Number of risk crisis response scenario playbooks completed
	Number of supplier BCPs completed
	Supplier BCP score, manufacturer and/or product resiliency scores over time

Risk monitoring and response	Number of potential disruption events detected/tracked Number of disruption events escalated for incident response Expected and actual TTR from major disruptions BCP completion by supplier (Note: Cisco collects 36 resiliency data points) Number of event escalations Event response time

Critical Success Factors and Best Practices:

- Completeness and reliability of metric data is critical for executive, program management, and stakeholder confidence.
- Technology that makes metrics reports easy to compose, understand, and share is critical.

1.5. Technology Plan

The next step is to figure out how the services will be managed and delivered. Table 6 provides (1) example functionality requirements for each service and (2) delivery mechanisms that are typically deployed to operationalize various SCRP service offerings.

TABLE 6. POTENTIAL SERVICE DELIVERY MECHANISM

POTENTIAL SERVICE	KEY FUNCTIONALITY	SERVICE DELIVERY MECHANISM OPTIONS
Risk intelligence	Supply network mapping and visualization Supplier data gathering, collection, and validation (survey) services	Software/cloud service Professional services for manual collection and follow-up Web-based process for data collection and analytics for validation
Risk analysis	Risk criteria/thresholds What-if scenario planning Risk quantification and scoring analytics	Software/cloud services

Risk treatment	Ownership assignment Resource and budget prioritization Risk mitigation progress/ metrics tracking	Shareable risk repository for high- and low-risk components/parts Internal standards and process development and execution Operational system/process integration
Risk monitoring and response	24X7 alerts War room capabilities	Email, social media, SMS Software/cloud services

Critical Success Factors and Best Practices:

- Involve users and partners in the requirements definition to encourage user buy-in and adoption.
- Be open to cloud-based SCRM offerings from niche born-on-the-web providers rather than megasuite vendors such as Oracle and SAP. There is no other option today.
- Ensure your technology infrastructure can leverage the latest SaaS, social media, big data/analytics and mobile technologies.
- Focus on rapid delivery of valued capabilities and aggressive change management since this is critical to achieving adoption.[7]

1.6. Program Office Team, Governance and Stakeholders

In this step the SCRP plan must address the various "who" questions. Who is going to deliver the service offerings that have been identified? Who is the customer for these services and to whom is the SCRP accountable for the delivery of these services? As such the team structure should (1) identify direct reporting relationships and dotted-line sponsors/champions and (2) define organizational structure and roles and responsibilities. Bear in mind, SCRPs, like all strategic initiatives require cross-functional participation, agreement and cooperation, as well as active executive participation and commitment in order to succeed.

Critical Success Factors and Best Practices:

- Identify and engage key players and stakeholders.
  - CPO or CSCO (overall accountability for supply chain resiliency)
  - Designated supply chain resiliency lead or "champion" (also typically serves as crisis response coordination and reporting lead)
  - Functional executive sponsors and stakeholders in the following departments:
    - Procurement
    - Manufacturing
    - Logistics

"No matter which delivery model and implementation style you use, the utilization of cloud/ SaaS will allow anticipated benefits of scalability and costs that cannot be achieved by using traditional on-premises models."

Christian Titze
Gartner
"Lessons Learned from 19 Supply Chain Visibility Initiatives"
January, 2015

- Engineering/product development
- Customer service
- IT vendor management
- Supply chain finance
- Governance, Risk and Compliance (GRC)
- Legal (import/export compliance)
- Designated functional core team members
- Commodity managers and process/program lead
- Manufacturing site leads and process/program lead
- Logistics managers and process/program lead

- Other stakeholders
  - Enterprise risk management
  - Supply chain IT
  - Business units (for customer communications)
  - Other supplier management, business continuity and security teams

> Define rolls and responsibilities for the central SCRM function, functional sponsors, and supply chain crisis response team (SC-CRT) members.

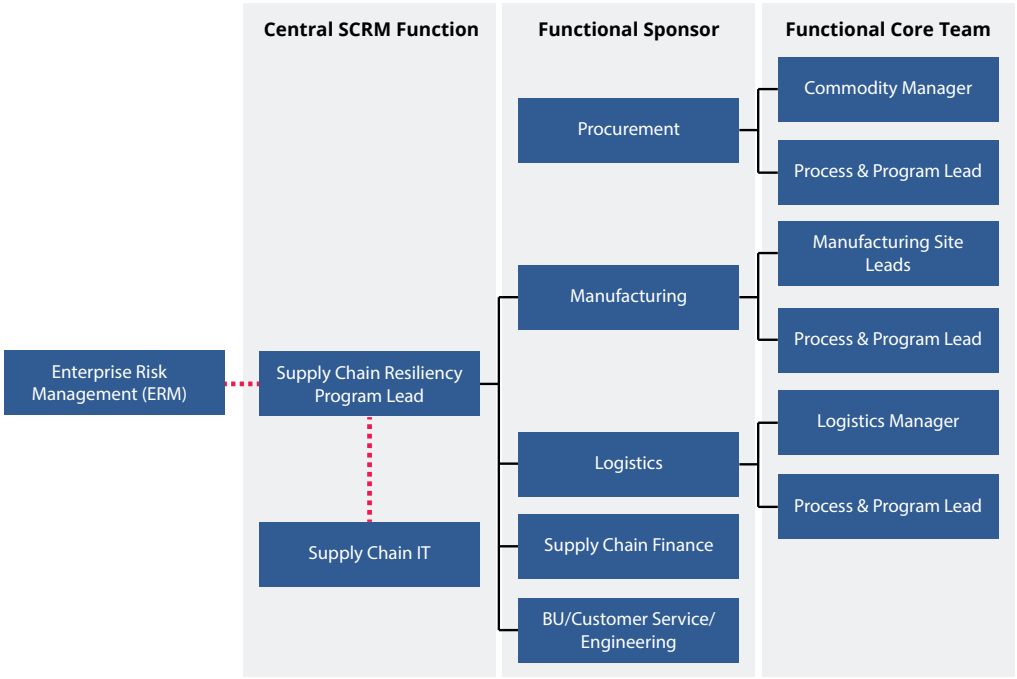
- Central SCRM function
  - Establish crisis alert levels and severity thresholds.
  - Establish activation criteria for crisis management process.
  - Conduct table-top drills to test BCP effectiveness.
  - Engage members of the SC Crisis Response Team (SC-CRT).
  - Establish communication protocols, war-room activation protocols, and ownership.
  - Develop crisis coordination infrastructure (war-room, bridge line, training material, SC-CRT badge).
  - Set up emergency budget and governance process with SC Finance and Functional Sponsors.
  - Lead coordination activities post activation.
- Functional sponsor
  - Provide executive sponsorship and designate and empower a crisis response lead for the function.
  - Participate in annual drills and table-top exercises.
  - Sponsor development of crisis response playbooks.
  - Provide functional input to the BCPs.
- SC-CRT members

Designating a single person responsible and accountable for your SCRP is one of the most important program critical success factors. Failure in this regard becomes especially apparent during a crisis.

- Represent the function on SC-CRT.
- Be on-call for events where the SC-CRT is activated.
- Understand roles, responsibilities and protocols.
- Attend SC-CRT training at least once a year.
- Get sponsor approval on roles and responsibilities and pre-approval for decision levels for faster crisis response.
- Participate in annual drills or table-top exercises.
- Promptly report in once the SC-CRT is activated.
- Act with appropriate sense of urgency in decision making and coordination.

- Operational staff (responsible for implementing mitigations)
  - Report on status.
  - Close-out mitigation project.

> Propose a team structure and engagement model. For a centrally organized SCRM function, the following model may serve as a template.



> Solicit and track stakeholder agreement to the SCRP team structure and engagement model.

> Ensure strong executive sponsorship and a relatively high reporting relationship with the company's management structure. Executive sponsors who are skilled in the areas in which the enterprise faces the greatest risk are the most effective.

> Drive towards a hybrid supply-chain organization which balances the extremes of

centralization, which promotes efficiency and controls costs, with decentralization, which provides flexibility and quicker time to market.

- Establish accountability for risk activities by designating ownership not by asset (these are the custodians), but by profit and loss leader, business manager, and product family owner.[8]
- Identify local contacts that can be empowered in the event of crisis, while still maintaining strong central coordination.

1.7. Timeline and Key Milestones

Of course, every plan must clearly identify key phases and milestones. This SCRP guide recommends at least three primary phases: Plan, Implement, and Institutionalize. Some major deliverables and milestones are suggested in the table below.

TABLE 7. TYPICAL TIMELINE AND MILESTONES

	PLAN "Storm"	**IMPLEMENT** "Form"	**INSTITUTIONALIZE** "Norm and Perform"
Time frame	0-6 months	6-18 months	18 months +
Objective	Define SC resiliency program	Roll-out SCRP (first iteration)	"Top 5" executive priority
People	Proposal for: > Governance > Customers/ stakeholders > SCRP team structure	Roles and job descriptions Awareness building Supplier communications	Risk governance/ exec leadership crystalized Regular executive/ stakeholder reviews Dedicated resources/crises team, category managers Supplier collaboration/ incentives
Process	Business case	Update business case	Expand business case
Scope	Initial program scope definition	Initial program scope implementation	Expanded program scope Risk data shared across all org levels, used in network and product design

	Business processes/ services definition	First iteration of SCRM services: > SC network map > Tier 1 supplier on-boarding > Risk identification > Risk analysis > Crises preparedness > Event monitoring > Incident response/ war room	Formalized processes (including change management), risk policies and thresholds Resilience program metrics and regular reports Risk used in supplier performance metrics Comprehensive supplier scorecards Comprehensive risk repository and collaboration hub
	Initial timeline/milestones (a version of this table)	Detailed 3-year plan in collaboration with system/ tool vendor	Maturity model
	Initial charter	Business plan	Updated business plan
Technology	System/tools plan	System deployment and training System/tools used for event monitoring, crises mgmt, risk identification, and BCP Tier 1 mapping	Analytics, revenue-based prioritization User/initiative footprint expansion System embedded in business processes and focused on pro-active mitigations N-tier network mapping

1.8. Program Funding

The SCRP program budget should include program management, headcount (internal, contracted, and any allocated headcount charges), and all incremental technology deployment and on-going support and maintenance charges. The level of funding for each category should take into consideration program scope and resulting in-plan SCRP services, as well as the service delivery time frame (i.e. a more aggressive roll-out schedule may require additional funding). Separately, funding may be required to mitigate risks or to support additional cost that could be incurred in a crisis situation.

Critical Success Factors and Best Practices:

- Benchmark and model headcount and technology needs against peer organizations, if possible.
- Use Cloud/SaaS technology platforms to minimize deployment, on-going costs, and IT dependence for roll-out timing, system administration/support, and upgrades.

1.9. Charter

Once all of the "why, what, how, who and when" questions have been answered, the organization is ready to publish and communicate its charter, which is essentially a high-level summary of this information.

Critical Success Factors and Best Practices:

The charter should contain:

- Concise statement of SCRP purpose and goals
- Definition of the scope and focus of the SCRP and target maturity level if applicable
- Definition of service offerings (aligned with SCRP scope and target maturity), service success criteria and metrics, and a high-level timeline of key service delivery milestones
- SCRP processes and a description of how the SCRP processes will be managed and delivered
- Description of SCRP organization structure and communications flow and a list of key personnel including SCRP sponsors and stakeholders
- SCRP funding requirements (estimate)
- Statement of SCRP authority and list of sponsor and key stakeholder signatories and/or charter approvers

2. Implement Phase

The implement phase is organized into three areas: People, Process, and Technology. The people section focuses on building the extended SCRP program organization including defining and staffing key roles and achieving the buy-in of the cross-functional team. The process section focuses on further refining the set of services the SCRP team will deliver and the initial implementation. The technology section focuses on system requirements and roll-out.

2.1. People

The first step in the implementation phase is to execute the hiring plan. With the high-level team structure defined, it is now time to refine key role definitions and job descriptions and begin the recruiting process for new roles.

Critical Success Factors and Best Practices:

- The most important role is, of course, the SCRP program director/lead (i.e. the "champion"). Key characteristics of the successful champion are as follows:
  - Respect for both leadership and staff
  - Knowledge of operations, processes, manufacturing, services, and intangible assets
  - Knowledge about risk assessment and management
  - Familiarity with high risk operation areas
  - Understanding of operations and the value chain
  - Capability to coordinate information flow from various sources
  - Appreciation for the dynamic and interdisciplinary nature of operations
  - Understanding of the organizational culture and change management processes[9]
  - Ability to form strong relationships and establish trust with stakeholders
- Additional roles and responsibilities should be defined in collaboration with the champion, if not driven by the champion.

Depending on the program scope definition, the team can evolve over time to include additional program management leads who are responsible for managing the various initiatives such as end-to-end visibility, proactive mitigation of components and materials, crisis response and recovery, business continuity, and capacity planning.

2.2. Process

The key to articulating and implementing the core SCRP processes is (1) providing clarity in terms of the overall process framework and (2) clarity in the definition and relationship between the various framework components. The challenge is that the various

processes, and terms associated with the processes, can collide and overlap. It quickly becomes confusing where one process starts and another stops. Further, the terms or labels for these processes used across methodology descriptions and even within the same source documents are not always clear. It is difficult to keep straight what the difference is between risk identification, risk assessment, risk evaluation, risk analysis, risk criteria, risk thresholds, risk appetite, risk scoring, risk mitigation, risk treatment, and so on.

The reality is that many of the lines between these process and terms are blurred and are difficult to untangle. For example, the process of supply chain mapping can be used to both identify and evaluate risks; risk "analysis" tools like the Bowtie method help with risk identification, evaluation, and treatment planning. This has resulted in the development of some inclusive best-practice guides that are comprehensive at the expense of being instructive.

The framework outlined below attempts to define and label processes in a way that makes them easier to understand, internalize and socialize. This approach better serves the objective of being mutually exclusive rather than collectively exhaustive. The result is a set of services that can be described as a series of 12 discrete steps. The reality is that in operation, the relationship between elements of many of these steps is more complex.

TABLE 8. POTENTIAL CORE SERVICE FRAMEWORK

STEP	PROCESS	KEY OUTCOME DELIVERABLE
Risk Intelligence		
1	Supply chain network mapping	Network map
2	Supplier/node data collection	Supplier information repository
Risk Analysis		
3	Risk identification	Risk register of vetted risks
4	Risk criteria	Evaluation parameters/metrics
5	Risk appetite/tolerance	Risk thresholds
6	Risk scoring	Priorities for treatment
Risk Treatment		
7	Risk mitigation planning	Completed mitigations/outcomes
8	Risk crises preparation	Crises response plans
9	Risk recovery preparation	Supplier business continuity plans

Risk Monitoring and Response		
10	Event monitoring	Real-time alerts and notifications
11	Supplier monitoring	Supplier visits/audits and change notifications
12	Risk tactical response	War room mobilization, post-crisis response postmortem

2.2.1. Risk Intelligence Service

Risk intelligence as defined here includes information associated with the supply chain network (i.e. relationships between nodes) that results from (1) the on-going supply chain mapping and update exercises and (2) the supplier/node information that results from the on-going supplier/node data gathering and information sharing exercises. Together they provide the basis for end-to-end supply chain visibility.

2.2.1.1. Supply Chain Network Mapping

During the implementation phase it is important to begin the process of mapping your supply chain focusing on the company manufacturing and logistics footprint and tier 1 suppliers. The ultimate goal is to create an end-to-end map as part of the risk management institutionalization phase. The mapping exercise yields the connections and relationships and dependencies between internal manufacturing and partner supplier sites. The node-level or supplier information (visibility) data gathering process is described next (see 2.3.1.2).

Critical Success Factors and Best Practices:

- Identify critical factories (owned, sub-contracted, sub-assemblies, ODMs).
- Document single source, alternate sites, and dual sources for critical products and parts.
- Map logistics hubs and alternative routes and providers for each major lane.
- Map products through supply chain and factories.
- Identify sub-tier dependency supplier names and global manufacturing footprint.
- Consider including critical indirect materials sources by first identifying points in the manufacturing process where tooling/equipment is needed. While doing so, identify critical equipment, tooling or consumables required in the production of high-revenue impact products and determine tooling constraints such as capacity, availability and replaceability.

2.2.1.2. Supplier/Node Data Collection

As part of the supply chain mapping exercise each manufacturing and partner supplier

node is then surveyed to gather risk profile information and evaluated to determine business impact (e.g. revenue dependency and spend). The result of both network and node-level processes is basic manufacturing and supplier visibility. An internal team can conduct the survey or an external service provider can provide the service as part of their supplier on-boarding service.

Critical Success Factors and Best Practices (for manufacturing and logistics information gathering):

- Document factory equipment and tooling.
- Document factory business continuity plans and develop the annual review and refresh process.
- Identify emergency response personnel and team trigger criteria.
- Assess BCP accuracy and level of reported training (e.g. have factory crisis drills been completed and results documented?).
- Clearly document first responder contact information and protocols.
- Identify cleanup and restoration vendor or note the need to put one in place.
- Collect information on previous site risk assessments to identify specific types of risks at specific locations and response plans for risks identified (e.g. crisis response plans for floods).
- Gather results of insurance audits for fire safety.
- Document recovery times, historical and expected supplier qualification times.
- Document key logistical processes, transactions, applications and system dependencies.
- Document manual logistics workarounds to keep material flowing in case of a systems outage.

Critical Success Factors and Best Practices (for supplier information gathering):

- Identify and document any supplier risk-related information related to planning, procurement, production, packing, storage, transportation, document preparation, reverse logistics, and information flows.
- For primary and alternate sites, determine recovery time, part origin, dual site/ alternative site readiness, and emergency contact.
- Identify n-tier dependency supplier names and global manufacturing footprint and map parts to global sites.
- Collect and asses supplier capacity information at a part level proactively (e.g. ability to add production lines and associated lead-times). Supplier capacity risk is one of several factors supply chain managers need to evaluate in order to ensure the uninterrupted flow of parts and products necessary to service fluctuating customer demand. A lack of visibility to supplier capacity constraints can directly lead to lost revenue and market share and declines in customer satisfaction and shareholder value if there is no capability to respond to supply shortages and

demand surges.

- Collect and assess business continuity plans (BCP) including a documented process and tested plan with trigger points and team training. Each BCP should address pandemic planning, emergency response and crisis management (process, team, internal/external communication plan), internal supplier risk assessment practices at the site level, and insurance coverage for contingent business interruption.
- Include in supplier site-level BCP surveys information related to BCP process, emergency response, crisis management & communication, transportation recovery (documented primary and alternative routes into/out of site), labor recovery (contingent labor workforce), safety (hazardous material handling, fire safety and prevention), security (authorized access into site), IT recovery (documented DRP, application inventory, IT redundancies, manual workarounds), backup power source and fuel supply, alternate site capability, and supplier's supply chain BCP information (i.e. efforts to make supply chain resilient).
- Upon completion of surveys, supplier BCP and site-level BCP plans should also include BCP scorecards, a process for BCP review and analysis, BCP standards and compliance requirement review, BCP data audit and data refresh, improvement and mitigation, QBR and metrics review, and resiliency incentive programs (e.g. new business awards, trusted partner program).
- In anticipation of the resiliency program institutionalization phase, prepare to perform data validation and refreshes to reconfirm and audit recovery times, validate alternative site information, validate BCPs, and refresh all Tier 1 mapping and part origin.
- For critical indirect materials:
  - Track ownership (self-owned versus partner owned).
  - Substitutes (if available), location, and current contact information.
  - Set acceptable thresholds for replacement lead times.
  - Negotiate lead time upfront.
  - Provide input to product design engineers regarding equipment/supplier selection and monitor supplier financial health to prevent NPI from leveraging tools from weak suppliers.
- Establish an auditable process including potential automation options for supplier change notification (e.g. change to an ingredient or raw material used in a sourced part or component, change in manufacturing location for a source component, etc.).

Consider leveraging social analytics that enable organizations to gather totally new information on suppliers, such as market sentiment and workforce attitudes, by maintaining a pulse on news and websites like Twitter and Glassdoor.[10]

"End-to-end supply chain visibility (E2ESCV) is a capability that provides controlled access and transparency to accurate, timely and complete plans, events and data — transactions, content and relevant supply chain information — within and across organizations and services to support effective planning and execution of supply chain operations "

Gartner

2.2.2. Risk Analysis Service

Once supply chain and supplier intelligence is gathered, risk analysis completes the tasks of identifying relevant risks, and evaluating those risks against a set of risk criteria and the risk appetite/tolerance thresholds to generate risk scores. Risk scores are then used to prioritize risk treatment activities and investment based on business impact.

2.2.2.1. Risk Identification

Risk identification is the more analytical process of determining broad categories of risks, threats, and vulnerabilities across your global supply network. It answers the question "what could go wrong?" and the result of the exercise is a list of relevant supply chain risks.

Risk identification is a pre-requisite to the risk scoring phase where risk quantification (i.e. likelihood, consequence and frequency) are determined for specific risk scenarios in order to prioritize risk mitigation or treatment investment options.

Many risks will have already surfaced as a by-product of the supply chain mapping process which provides a visual representation of the supply chain network, connections, dependencies, bottlenecks, and potential single-points-of-failure that could represent unacceptable risk.

Other methods include historical analysis, industry trend research, and brainstorming. Further, direct supplier information gathering approaches can be employed such as surveys, site visits, and data system audits.

Too many organizations launch a resilience program without a clear understanding of what the keys risks are and what consequences a disruption would have. As a result, they focus on the wrong threats rather than those that matter. These organizations might fail to recognize the consequences of an apparently minor threat.[11]

Critical Success Factors and Best Practices:

- Develop an initial risk register to identify baseline risks (at the global network and regional/location level).
- Ensure that all key stakeholders are represented on the risk identification team.[12]
- Establish some basic parameters for determining what qualifies as a supply chain risk, vulnerability or threat that should be considered for more detailed evaluation. Minimally, risks that should be considered are those that could prevent the organizations from achieving key or strategic objectives and financial goals.
- Use a variety of lenses to identify/segment risks such as:
  - Strategy risks (e.g. failure of a strategic product/market entry launch)
  - Product/part/component risks
  - Supplier risks
  - Supply network risks

- Incident type risks
- Geographic supply chain risks
- Demand volatility risks

> Ultimately, however, view all risks through a business value lens. This typically leads to a focus on product families and aligned suppliers producing the greatest revenue, margin, cash flow, etc. The power of this approach is that execution is more focused because of the "80-20 rule" which, in this case, refers to the fact that typically 80% of a company's revenue or profit is driven by 20% of its products or is dependent on 20% of its suppliers. However, the approach needs to be flexible to accommodate exceptional scenarios (e.g. new strategic products without a revenue/profit history).

> Note that programs that identify risks through an individual resource or asset lens (piece of machinery, plant, warehouse)[13] or an incident/causal lens (e.g. vulnerability or threat scenarios such as "What if there is major earthquake in our San Jose headquarters location?") have been less successful in securing on-going program support.

> Keep in mind that normal variations in product demand and quality, and those that are maintained within acceptable limits, do not represent risks that should be included in the resilience management process.[14]

> Review against a comprehensive list/taxonomy of supply chain risks. The SCLC "Supply Chain Risk Management: A Compilation of Best Practices" August, 2011, provides an exhaustive list of supply chain risks in the Appendix.

> Be aware that risk identification is a function of local conditions and may vary from site to site within the same organization as well as between supply chain elements. As a result, it is essential to identify the risks associated with locations and functions and choke points in the supply chain.[15]

> Complete an internal best practice evaluation of risk identification tools and methodologies. These include:

- Simple Pareto or more sophisticated portfolio analysis (i.e. to determine which product families, products, parts/components and suppliers are associated with the highest business value and business continuity risk)
- SC Risk Identification Structure (SCRIS) tool developed by the Council of SCM Professionals[16]
- War game scenario planning simulations (e.g., what would happen if a major port was shut down for an extended period of time?)
- Single point of failure (SPOF) analysis[17]
- Risk checklists (based on past experience or industry research)[18]
- Cause-and-effect diagrams (i.e. fishbone, Ishikawa)[19]
- Gantt charts to identify critical paths/bottlenecks can also be used in risk assessment to determine effect of disruption at different points in the supply chain

2.2.2.2. Risk Criteria

For individual risks surfaced in the risk identification process, risk criteria serve as the benchmark or scales for the evaluation and measurement of risk consequences and likelihood. The risk scores against these criteria will be used to prioritize risks for risk mitigation. Risk criteria can be qualitative and quantitative as well as represent both real and perceived risks.[20] Examples of risk criteria include impact to key business metrics such as revenue, costs, and customer satisfaction or pose specific risks to supply chain continuity and operations such as supplier financial, location, recovery or capacity vulnerabilities.

Critical Success Factors and Best Practices:

> Define risk scoring risk categories and category criteria. Key risk categories and criteria include:

- **Financial Risk**. Risk score is at the supplier level including:
  - Financial health
  - Credit risk
  - Z-score
  - Debt rating
- **Location Risk**. Risk score is at the site level (i.e. a single supplier would have multiple locations globally and each one of those sites would have its own location risk score). The scores for each site should roll up to an aggregate supplier level location score. This aggregate view could be a maximum, average, or a weighted average score. The aggregation approach can vary by company based on philosophy and approach. This can encompass:
  - Natural disasters
  - Geopolitical
  - Macroeconomic
  - Local facilities, safety practices, infrastructure, etc.
- **Recovery Risk**. Risk score is at the supplier, site and part level. A single supplier could have multiple parts manufactured at the same site, and a separate recovery score for each part and site combination. A single part could be manufactured at two or more sites in a multi-step process, in which case the same part could have a separate recovery time for each individual site. Scores may be rolled up to the supplier level and site level. For a given part, redundant manufacturing or readiness of an alternate site is adjusted in computing recovery risk score.
  - Recovery time
  - Business continuity plan
- **Operational Risk**. Risk score is at the supplier, site and part level including:
  - Delivery reliability

"While there are many different sources of risk to consider, there are a very limited number of outcomes (e.g. loss of supply capacity, internal operational disruptions, transportation delays, unplanned human/financial resource spend, etc.). As a result, there is more leverage in planning for the system to be resilient in response to the predictable few outcomes."

Jim Rice
MIT

- Lead-time performance
- Quality
- Cost Performance
- Flexibility
- Trends

- **Sourcing Risk**. Risk score is at a part level including:
  - Single sourcing versus multi-sourcing
  - For a multi-sourced part, the split allocation between sources can be considered in a risk score

> Note that risk criteria require on-going monitoring and re-validation against current operating environment assumptions. For example, during a period of financial uncertainty, the financial risk score of suppliers may be weighted higher than other risk parameters.

2.2.2.3. Risk Appetite/Tolerance

Risk appetite and tolerance characterizes the boundaries for the appropriate amount of risk taking within an appropriate level of authority. It drives the decision regarding whether or not a risk should be accepted, treated, and re-treated as a result of residual risks. For suppliers, risk thresholds can be set for the supplier as a whole or at the individual risk category and category criteria level described above.

Critical Success Factors and Best Practices:

> Consider leveraging risk frontier graphs and heat maps to visualize and conceptualize the boundaries between acceptable and unacceptable risks based on likelihood and consequences.

> Determine the risk policy, thresholds, and exception management process.
  - Set risk policies to balance cost savings and other financial targets with resiliency objectives and projected benefits.
  - Set risk threshold tolerance limits by commodity, product, sourcing, impact, recovery time, risk scores, and supplier types.
  - Implement exception management approval rules (e.g. dual source suppliers responsible for more than 75% of the supply of a high-impact part require approval) and approval level limits (e.g. exceptions requiring VP versus manager level approvals – can be by exception type).

> Define specific risk threshold/policies (i.e. "risk appetite") by function. While risk thresholds can be set based on many different criteria as defined below, revenue impact may be the primary or only criteria necessary for a given function.
  - For raw materials/components:
    - Set threshold/rules for suppliers, parts and/or by commodities.

- Set threshold/rules based on recovery time, financial impact, product, or financial, location, or sourcing risk score. Examples of risk threshold rules include:
  - A part that impacts more than a set revenue threshold cannot remain single sourced.
  - A financial risk score cannot be higher than a set threshold.
  - Recovery time cannot exceed a set threshold number of weeks.

- For manufacturing:
  - Set recovery time for manufacturing sites.
  - Set risk scores for manufacturers and sites for sub-contractor-owned manufacturing.
- For product:
  - Set new product release criteria.
  - Set a minimum part/supplier threshold.
  - Note: Extensive product release gate exception processes can be at odds with time to market or other company objectives. For example, revenue impact in this case can be "products which are expected to replace highest revenue lines."
- For equipment/tooling/consumables:
  - Set supplier financial risk scores for critical equipment vendors.
  - Set lead time for replacement equipment.
  - Note: This may be difficult to implement for every piece of equipment. Therefore, revenue impact can be used as a threshold. For example, a rule can be established that any product lines exceeding the threshold are required to undergo the formal risk assessment process.
- For IT and critical application systems:
  - Set recovery time objectives (RTO) in hours/days for priority 1 (P1) and priority 2 (P2) applications.
- For logistics:
  - Set the number of logistics providers or hubs for a given lane based on a given revenue impact threshold.

2.2.2.4. Risk Scoring

Risk scores assess the likelihood, frequency and consequence (e.g. revenue impact) of risks facing a company and then use that information to prioritize risk exposures for mitigation. Subjects of risk scoring include suppliers, sites/locations, products and parts. A time horizon is necessary to characterize the probability of risk in a useful way. Risk scores enable the supply chain resilience team to focus on the efficient, rapid allocation of investment dollars against these exposures. The result of this phase is a list of critical

vulnerabilities which have the highest risk score – and therefore, have the highest priorities for supply chain risk management attention.

The job of risk scoring is predicated on having a set of identified, vetted risks, a set of risk categories/criteria and associated thresholds, a formula for calculating an aggregate risk score (e.g. a simple weighted average), as well as a set of consistent user guidelines for scoring vulnerability or threat scenario intelligence against the scoring criteria. The job of developing a risk scoring formula and methodology frequently falls on the SCRP and is usually, therefore, considered proprietary or semiproprietary by program owners. It is more likely that a basic methodology will be promulgated by a consulting services or technology solution provider. However, since every organization and supply chain network is unique, do not expect to be able to leverage an external publicly shared "best practice" standard formula (i.e. set of criteria, weighting, etc.).

Regardless of how it is accomplished, risk prioritization is imperative, first, because one cannot insure against all risks; risk transfer is too expensive. On the other hand, one cannot rely solely on being reactive since the level of exposure and vulnerability may not be acceptable -- nor is this a responsible way to operate the business. Further, all risk should not be proactively mitigated as this is too resource intensive and not cost-effective. Nor can all risks be accepted since this leaves an organization too exposed. The key is to find the right balance between the benefits of proactively protecting supply continuity and reactively responding to a crisis.

A holistic and programmatic approach to risk identification, quantification, prioritization, and review described above can enable practitioners to make decisions about risk treatment, balancing acceptance, mitigation, and transfer costs with business cases and other considerations.

Critical Success Factors and Best Practices

- Weigh the benefits of a risk prioritized for mitigation against the cost/resources investment required to mitigate the risk. The risk investment must be justified based on a quantitative assessment of the business value at risk and the impact of failure. Long gone are the days of trying to sell the risk program based on qualitative judgments.[21]
- Define supplier risk scoring analytics for key supply network nodes. This typically focuses on suppliers or logistics hubs with highest consequences of disruption based on revenue impact (e.g. single source locations, suppliers/logistics hubs that touch a large part of the product portfolio) and integrating risk likelihood and frequency information. Based on a pre-defined matrix of customized risk categories and category criteria, weighted average calculations then combine consequence/impact and likelihood/frequency scores in order to prioritize supplier risks for mitigation.
- Design scoring processes that properly weighs frequency of occurrence. A common misstep is placing too much emphasis on the highest impact risks. Supply chain impact research indicates that smaller, more frequent disruptions are more costly in aggregate than those precipitated by high-impact, but infrequent

events.

- In segmenting/scoring suppliers, weigh revenue impact versus spend appropriately. A common mistake promulgated by "strategic sourcing" strategies and systems is to focus on the 20% of the suppliers that constitute 80% of the procurement spend. This could result in a low-spend supplier of a single-sourced part for a high-revenue part off the radar for risk management attention.
- Take into consideration what type of information is readily and reliably available to compensate for data gaps (e.g. financial data for private companies) and to incorporate a means for periodic auditing of third-party information validity.[22]
- Experiment and try out a scoring methodology on key/critical suppliers and be willing to tweak and/or switch out the methodology if it isn't able to accurately discern the level of risk or deliver reliable enough information.[23]
- Consider and evaluate the role that various risk assessment and scoring methods may play in complementing your process, as well as validating/testing your risk evaluation and prioritization conclusions:
  - **Supplier segmentation** segments supplier by revenue impact or other business impact measure and uses that to prioritize individual supplier remediation investments.
  - **Risk exposure index** is a supplier segmentation method that focuses on supplier time to recovery (TTR) in a major disruption scenario. Every node in an end-to-end supply chain is evaluated to determine the financial impact in order to rank suppliers for mitigation investments.[24]
  - **Failure mode and effects analysis (FMEA)** prioritizes risks based on (1) seriousness of consequence, (2) likelihood of the problem occurring or frequency, and (3) likelihood of early detection of the problem.
  - **Scenario planning** models complex supply chains and stress tests the cause and effect nature of any a "what-if" scenarios within the supply chain and yields a dashboard of prioritized scenarios and associated risk response plans.
  - **Residual risk analysis** is used to evaluate risks before and after a risk mitigation. If the likelihood and consequence of residual risk is greater than the established risk tolerance, then further risk mitigation is required. Assessing risk tolerance can be facilitated by using a risk frontier graph which plots the likelihood of events by their consequences.
  - **Risk heat maps** can also be used to assess and visualize risks by categorizing risks on a scale of likelihood and consequence.[25]
  - **Probabilistic simulation and modeling** is a supplier location-based analysis of high risk and consequence nodes based typically on maximum loss value or revenue at risk. Success of this approach depends on clearly articulated end goals/objectives, expected outcomes and application of results, reliable probability data, and well understood impact and severity scenarios. This best practice is typically recommended for sophisticated practitioners of stochastic simulations and limited to direct manufacturing and/or outsourced

manufacturing locations.

- **Fault tree analysis (FTA)** is concerned with analyzing faults or the multiple causes which might lead to an event and identifying preventative measures.
- **Event tree analysis (ETA)** is interested in stopping event consequences from escalating by identifying and mitigating the impacts. When used in combination these tools are referred to as the Bow-tie Risk Analysis Method linking treatment of risk to cause and consequence.
- **Net present value (NPV) analysis** can be used to quantify the financial impact of a supplier failure and prioritize suppliers for mitigation.

2.2.3. Risk Treatment and Response

Risk Treatment and Response		
7	Risk mitigation	Completed mitigations/outcomes
8	Risk crises preparation	Crises response plans
9	Risk recovery preparation	Supplier Business Continuity Plans

Now that risks have been assessed and prioritized, remediation measures need to be identified and implemented for events that have not yet materialized. This includes risk mitigation planning to address the specific product/part and supplier vulnerabilities addressed in the risk analysis phase, general crises preparation to address risk more systemically, and risk recovery plans (i.e. damage control) to ensure consequences are contained after a supplier incident has occurred.

The SCRP supports the development of these pre-event mitigation plans. It is typically the operations team's responsibility to execute on the risk recommendations and plans developed by the SCRP team. Risk mitigation or risk treatment, per ISO Guide 73:2009, measures include:

> Removing the risk source (e.g. product design for resiliency)

> Changing the likelihood (e.g. network design for resiliency)

> Changing the consequences (e.g., proactive mitigation planning, crises preparedness, alternate sourcing)

> Sharing or transferring the risk with another party or parties (e.g. supplier contracts, risk financing/insurance, vendor managed inventory, supplier collaboration)

> Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk

> Taking or increasing risk in order to pursue an opportunity

> Retaining the risk by informed choice

Risk treatments that deal with negative consequences are frequently referred to as risk mitigation, risk elimination, risk prevention or risk reduction. Note, also that risk treatment can create new risks or modify existing risks.[27] The optimal response must consider the cost-efficiency of the alternative measures.

"Low spend parts and suppliers can have high impact. You can't ship a coat with a missing button or an appliance with even a missing sticker. Every single part is important."

Joe Carson
VP Global Operations Excellence
Juniper Networks

2.2.3.1. Risk Mitigation

Risk mitigation here refers to the proactive measures undertaken to remedy the risks identified, assessed, and prioritized during the risk analysis phase. In addition to the selection of the mitigation approach, risk mitigation includes the important processes and tasks associated with setting mitigation targets, getting approval for costs incurred, tracking mitigation activities in progress, reporting on status, and closing out the mitigation activity.

It is also important to address the staffing related question such as who manages and executes the mitigation efforts (typically operational teams) including all of the processes and tasks stated above.

Some mitigation remedies can be implemented in the near term and some options may not be available for consideration until the program is more mature (i.e. reaches the institutionalization phase). A partial list of options – roughly ordered from near- to long-term implementation lead time – include:

- Inventory/safety stock management and daily (control tower) monitoring
- Forward buying or hedging to mitigate cost risks
- Closer collaboration/planning with suppliers (Tier 1, 2)
- Active supplier monitoring combined with early detection
- Alternate or redundant/dual sources and site qualification
- Contract management including risk sharing and performance-based contracts
- Supplier BCP standards
- Product design for resiliency including component substitution and postponement or delayed differentiation strategies
- Network design for resiliency
- Product portfolio rationalization
- Pooling inventory across companies and creating virtualized and shared inventory management systems to improve parts availability
- Regional diversification of distribution centers
- Regionalizing production and distribution to accelerate the matching of supply with demand and help lower the risks of long transportation lead times
- Near-shoring
- Vertical integration

Framework for Choosing Mitigation Strategy for High Impact, Single Sourced Parts			
Financial Risk	Location Risk	Recovery Risk	Assess mitigation cost, time to switch to alternate source & other considerations
HIGH	LOW	LOW	> Second Source > Cover short term demand with inventory
LOW	HIGH	HIGH	> Alternate site readiness > Improve recovery risk
LOW	HIGH	LOW	> Inventory to cover recovery time
LOW	LOW	LOW	> Lower priority for mitigation > Cover recovery time with inventory

The framework above addresses mitigation choices which are in line with the decision to "do something". After considering the cost of mitigation, risk thresholds, available budget, resources, complexity of implementing a mitigation, and other priorities of the business, the optimal decision could very well be "do nothing" by informed choice. The important distinction between an informed decision to "do nothing" contrary to "do nothing without proper analysis" is that in the latter case, the business is operating blind. Without a proper identification and analysis of supply vulnerabilities it takes longer to assess the impact and develop and mobilize an optimal response plan.

In the life sciences industry, qualifying a new supplier can be a 3-6 year process due to regulatory policies. Thus, diversifying the supply base can be prohibitively expensive, but the risk of sole sourcing can be equally unacceptable. To address this conundrum Genentech undertook a detailed NPV analysis of its supplier base to score suppliers for mitigation prioritization.[26]

Critical Success Factors and Best Practices:

- Basics
  - Monitor risk thresholds and exceptions.
  - Establish owners by supplier/part/product.
- Mitigation selection and execution
  - Adopt a framework for choosing appropriate mitigation strategies.
  - Define a business justification methodology and template for reviewing and approving mitigation related costs.
  - Plan to conduct mitigation budget justification and approval process/meetings on a periodic basis.
  - Note that mitigation strategies may need to vary significantly based on a product's core value driver which can vary from quality, to price, to innovation to availability, to customer experience, and so on. For example, a product that is differentiated by innovation may correlate with lower forecast accuracy, and higher price and supply risk as a result of the speed of innovation. It is more likely that flexible risk-sharing contracts, rather than a build-up of inventory buffers, is appropriate. On the other hand, if availability is a key value driver, inventory buffering is a more logical response. Thus, the risk treatment approach may need to be segmented according to the value driver.[28]

- Mitigation targets, metrics and incentives
  - Develop quarterly mitigation targets and metrics.
  - Implement incentive plans for proactive mitigation execution.
  - Create a plan to integrate mitigation progress reviews into every operational review meeting at every level of the organization.

Note: Several of the recommendations listed in the two bullets immediately above may not be fully operationalized until the program moves into the "institutionalization" phase described in Section 3. They are surfaced here because it is useful to start considering some of these potential next steps in the planning phase.

2.2.3.2. Risk Crises Preparation

Your crises preparedness plan should include seven primary activities:

1. Determine the crisis team roles and responsibilities and governance.
2. Define communication channels.
3. Establish event response-level triggers.
4. Develop and document playbooks.
5. Map and develop IT/application/system recovery processes.
6. Develop a post-crises assessment and continuous improvement process.
7. Define and test the basic processes.

Critical Success Factors and Best Practices:

- Determine and develop the crises response team roles and responsibilities and governance.
  - Designate a leader responsible for crisis coordination. The CPO or CSCO should have overall accountability, depending on the scope of the SCRP. The leader can be designated by the person who has overall SCRP accountability. The leader should be a director-level individual or above, who has demonstrated strong leadership, cross functional efficacy, a strong sense of ownership and urgency, and the ability to remain calm under pressure.
  - Identify and designate a program management lead who can operate at the people, process, and technology layers to bring together various elements of the SCRP.
  - Empower the extended team to make decisions locally without lengthy analysis. This requires a supply chain model structure that is flexible, meaning that there is decentralization when required with strong central control.[29]
  - Identify, engage and regularly train members of the SC Crisis Response Team (SC-CRT).

- Establish the supply chain war room infrastructure. Set up activation criteria and develop a training program for all members of the SC-CRT. This can include a conference room designated as the SC War Room (modeled along the lines of an executive briefing center), including a bridge line, special SC-CRT security badges, and instructions (e.g. manual of standard operating procedures).
- Determine the decision makers for any response budget needed and set up the emergency budgeting and governance process with SC finance and functional sponsors.
- Collaborate with the Enterprise Risk Management Team (ERM) to coordinate and synchronize SC-CRT roles and responsibilities and protocols with the corporate team. The SC-CRT plugs into the Corporate Crisis Management Center which is responsible for the overall company response to a crisis event. Their scope includes impact to people, company-owned buildings and property, and non-supply chain locations and concerns.

> Define communication channels.

- Establish the protocol and owners for notifying CxOs and customers.
- Pre-define direct communication channels up, down, and across the organization as necessary with the functional and domain experts who can best help identify risks and take appropriate actions and handle specific scenarios and situations.
- Ensure suitable communication methods are defined (e.g. phone, email, SMS, social media, etc.) to ensure speed, reliability, and as appropriate, redundancy and auditability.
- Determine media relations procedures.

> Establish event notification and response activation triggers to direct an appropriate, proportional response.

- **Level 1**. Notifications that are to be treated as a "FYI."
  - Impact is not likely to be felt for more than a few hours or days or pertains to an area with less significant business dependency.
  - Duration falls within the risk threshold.
  - People need to be aware just in case the situation deteriorates.
- **Level 2**. Notifications that are placed on the company "watch" list.
  - Situation is evolving – might be resolved, but there's a chance it could deteriorate.
  - Evasive action might be very expensive and wasteful if not required.
- **Level 3**. Notifications that are to be "researched" for potential impact.
  - Impact may be felt – more information is needed about supply chain dependency on the region/supplier/site.
- **Level 4**. Notifications that require some preventive action.

    - Potential for impact is real – based on initial research or notification itself, it is clear that supplier(s) may be affected.
    - The cost of doing nothing outweighs the losses incurred if the worst case scenario plays out.
  - **Level 5**. Leadership needs to be "woken up" to be notified.
    - Impact is real and immediately obvious
    - Customers, executives and media/analysts will immediately begin asking questions

> Develop and document playbooks.

  - Document actions and strategies ("playbooks") that will be mobilized for different activities in the case of an event.
  - Account for the unique characteristics of make-to-stock versus complex engineer-to-order supply chains when developing playbook templates for common supply chain disruptions.[30]
  - Identify top 5 supply chain hotspots for event-based playbooks (e.g. Japan Earthquake, Thailand flood, etc.).
  - Identify required risk data for the playbook scenario (e.g. number of sites and parts from region, revenue impact of parts, recovery time, etc.) and establish risk acceptance levels, clear mitigation options, and crisis response actions.
  - Identify owners and processes for re-locating people, systems, and data; transferring operations to alternate sites; and bringing impacted IT systems and applications back online.

> Map and develop IT/application/system recovery critical to getting orders and products shipped in order to ensure recovery time objectives (RTOs) for supporting technologies are met.

  - Identify critical P1 processes, applications and systems (including hardware) that are needed in order to receive an order, enter it in the system, place the component orders in the appropriate lead-time windows, receive parts in, drop a kit, complete the manufacturing steps, process shipments for each site and manufacturing process, and recognize revenue.
  - Set recovery time objectives for all the processes above. Recovery time objectives should be aggressive, and incorporated into the contracts with each vendor touching the application, middleware and infrastructure layers supporting the critical processes. This is especially important where manual workarounds are not available or possible.
  - Document manual workarounds for key P1 applications and processes.
  - Document people in the organization who have been trained on the manual workarounds. Maintain a live document with an annual review of the emergency plan.

> Develop a post-crises assessment and continuous improvement process. Every

crisis (whether impactful or not) is an opportunity to learn and hone the process and tools. It is very difficult for a company to put a system or process in place during an event.

- Determine an owner who is responsible for coordinating and driving the post-crises review and addressing subsequent gaps and areas for improvement by working with the appropriate function.
- Determine review participants in the assessment.
- Create a post-crisis assessment checklist (example checklist follows).
  - How quickly was the event detected?
  - Were the war room activation performed on time?
  - Did the triggers work?
  - Did the infrastructure and tools work?
  - Was the mapping information helpful?
  - What information gaps were experienced?
  - Were training gaps exposed?
  - Was the budget released in a timely fashion?
  - Was the governance process effective and responsive?
  - Were proactive mitigations helpful in averting a major impact?
  - Did suppliers communicate and support effectively and in a timely fashion?
  - Did we or suppliers perform according to the BCP?
  - How did executive or customer communication get handled?
  - Did crisis preparedness measures help?
  - How can we change the process to address these gaps in future?
  - What was the time and cost of recovery?
  - What was the resource utilization and overtime impact?
  - How many people, how many days or weeks, how many hours per day?
  - How much did we pay in premiums and freight expedites?
  - Did ongoing activities suffer when resources were diverted (opportunity cost)?
  - If commodity managers were diverted into response, what is the dollar impact to cost savings target achievement that quarter/year?
  - Did we experience lines down? How many days, how many lines?
  - What was the cash burn from lines down?
  - Were OTS or other metrics impacted?
  - Was revenue impacted? How many days or weeks?

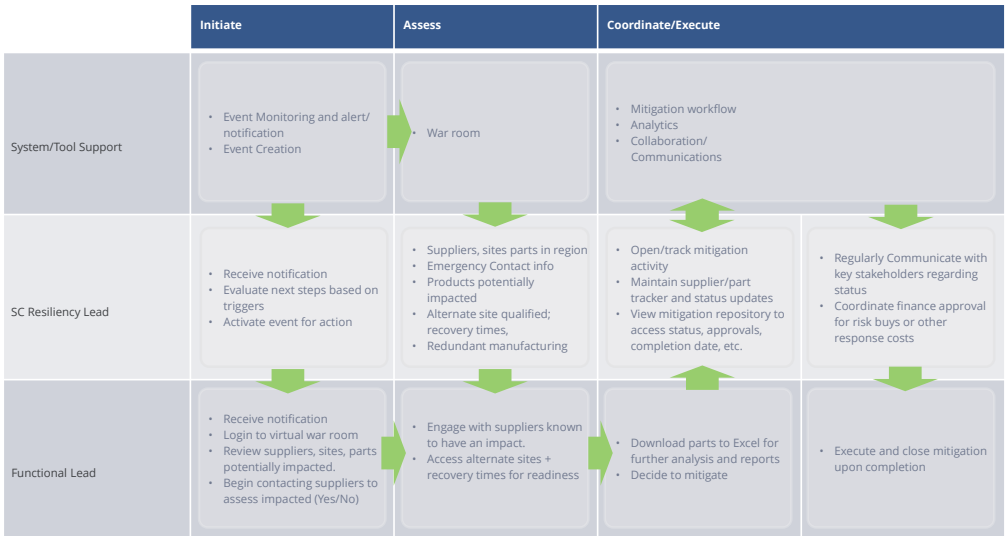
- What was the overall time and cost to recover from the event?

> Define and test the basic processes.

- Establish crisis alert levels and severity thresholds.
- Establish activation criteria for the crisis management process and BCP.
- Conduct table-top drills to test BCP effectiveness.
- Develop the crisis coordination infrastructure (war room, bridge line, training material, SC-CRT badge, playbooks).

Answers to the above questions can help the company further develop and update the return on investment analysis from an investment in the SCRP program, technology and resources. This may be vital when program budgets need to be re-justified and renewed or expanded.

The following graphic summarizes the event crises response life cycle by key roles and activities.



2.2.3.3. Risk Recovery Preparation

Risk recovery preparation focuses on contingency planning that ensures production and product delivery continues — either uninterrupted or with minimal financial, competitive or customer impact — in the event of a supply chain disruption. Supply chain business continuity planning (BCP) is the vehicle for preparing the business and its network of supply chain partners, so that they perform continuously regardless of where and when a supply chain event occurs.

Critical Success Factors and Best Practices:

> Build a cost-effective and repeatable survey process for assessing supplier business continuity risk and recovery capabilities at the part level.

- Centralize that information into a comprehensive supplier risk evaluation and mitigation repository or hub (i.e. do not build a separate data repository for risk, BCP/recovery data, and capacity information).
- Leverage the data collection and update process used to gather risk intelligence to simplify supplier participation and response efforts.
- Invest in analytics to drive supplier scorecards, revenue impact analysis, and risk mitigation strategies and tactics.

Remember, an informed and proactive choice to "not mitigate" a risk that ultimately results in a crises is better for crisis response and recovery, than an uninformed organization that blindly marches into the unknown without an idea of what the potential impact could be from a given event.

2.2.4. Risk Monitoring & Response

Once mitigations have been applied, on-going constant event and supplier monitoring is required to ensure that risks have not exceeded established tolerances. This is especially important given that it is not practical to mitigate all risks proactively. Tactical responses are then mobilized once an incident has occurred.

Risk Monitoring and Response	
Event monitoring	Real-time alerts and notifications
Supplier monitoring	Supplier audits and change notifications
Risk tactical response	War Room mobilization

2.2.4.1. Event Monitoring

Once your basic crises preparedness plan is in place and response level triggers are in place you are ready to deploy a multi-tier real-time event monitoring service to detect and respond to potential threats, mobilizing "playbooks" as appropriate and/or war room capabilities (described next).

Event monitoring services of varying levels of robustness are available from third-party service providers or as a component of an integrated SCRM system. Event monitoring services should be used to complement supplier monitoring services (e.g. financial health) conducted by internal users leveraging external services.

Critical Success Factors and Best Practices:

Implement a best-in-class event monitoring service that supports the following capabilities:

- 24X7 event notification distribution via email, social media subscription or other delivery vehicle.
- Consolidated and summarized event notifications and alerts including size, scope and potential impact to specific customers, industries, geographic areas, and parts/components.
- Alerts on a comprehensive array of event types such as natural disasters, factory

explosions, labor disputes, power outages, chemical spills and geo-political upheaval.

- Alerts on non-catastrophic but disruptive developments in the supply chain due to mergers and acquisitions, government regulations, punitive action against a supplier or factory due to non-compliance to local laws.
- Monitoring of all information sources including news and social media sources; company financial sources; industry sources; executive and biographical sources; public records; government sources; as well as in all major languages with UN, EU, and APAC monitoring.
- Intelligent event filtering that removes redundant and irrelevant/non-impactful events.
- Integration with a supply chain risk management (SCRM) platform in order to map automatically disruptions detected with potentially impacted suppliers, sites, products, parts and associated revenue.
- A supplier notification process whereby suppliers can notify the company about events that they are impacted by. This ensures that appropriate individuals are quickly notified when a supplier problem is not picked up by the monitoring service. Ensure there are multiple individuals on the company contact list in case one contact is unavailable to receive or respond to the message.

2.2.4.2. Supplier Monitoring

Several tools and approaches for continuous supplier monitoring may be appropriate given your organizational context including collaboration/information sharing processes and tools, audits, metric tracking, and contractual terms and incentives.

Critical Success Factors and Best Practices[31]:

- General
  - To the extent possible, make routine site visits to ensure workplace practices and product quality are consistent with expectations and to increase the likelihood of early discovery of potentially major problems.
  - Consider investing in local advisors in countries where suppliers are operating to provide early warning on political or economic risks to suppliers – such as imminent strikes or government nationalization of suppliers – and to neutralize any potential issues introduced by a lack of understanding of local cultural dynamics.
  - Ensure supplier audit/scorecards include strategic risk metrics (financial scores, location scores, recovery, and BCP targets in addition to operational metrics).
  - Keep in mind that the earliest signs of a pending supplier crisis often manifests as compromises on quality or delivery.[32]
  - Track and monitor time-to-recover (TTR) at the part and site levels at the

manufacturing component or test level as appropriate.

- Keep a continuous watch on part-level supplier capacity in case projected 12-month demand is too close to the maximum available capacity for a given supplier. Early warnings and system-generated alerts about these bottlenecks can provide critical incremental reaction time before other industry players begin to vie for available capacity.
- Maintain an alert system for part change notifications. Sometimes these can create major disruptions for companies, especially if a major part change or end of life is declared on a high-revenue-impact part.
- Leverage web-based and industry standard evaluation/audit tools (e.g. Supply Chain Leadership Council; www.scrlc.com).
- Consider planning crisis drills with key suppliers each quarter to test BCP plans, effectiveness, and timeliness of communications and adherence to TTR metrics.
- Conduct quarterly business reviews (QBRs) that drive improvements in the BCP and visibility coverage.

> Contract terms

- Include language in supplier contracts for timely notification and regular status updates in case of a disruption. Specifically, the business continuity and the force majeure clause should include language holding suppliers to their BCP and recovery time objectives during a force majeure event to strengthen accountability (i.e. make BCP delivery a mandatory requirement per the contract).
- Include a supplier visibility and transparency clause that makes visibility a requirement for suppliers by inserting language in the contract that obligates suppliers to disclose critical sub-tier dependencies as well as provide manufacturing site visibility.
- Include service level language in the contract that requires suppliers to provide notification within a specified time period of a major event impacting the supply chain.

> Incentives

- Use incentives to reward suppliers for developing and implementing policies specifically focused on minimizing risks proactively.
- Provide incentives for suppliers that pass a supplier recovery time/BCP audit, meet minimal acceptable BCP standards, or meet targets in a crisis. Examples of incentives that drive the right behavior include:
  - Favorable scoring on supplier scorecards than can lead to preferential treatment
  - Trusted, Preferred or Strategic Partner status awards
  - Condition for new business awards

- Condition for securing on-going business

- Consider providing negative incentives. While positive incentives are ideal and preferable, in cases of severe non-conformance, negative incentives may need to be implemented. Some examples are putting suppliers on a performance improvement plan and shifting volume to other suppliers. Without such consequences, the SCRP efforts may not be taken seriously by suppliers.

> Change notifications

- Review efficiency of change notification process. This process is typically extremely manual, slow, and difficult to track/audit. Additionally, if a supplier changes a key part with high usage across the product portfolio, this can cause a major effort to either redesign products to support the change or result in the need to place an expensive life-time buy for a part if an alternate cannot be qualified. This represents a huge risk to supply chains and associated revenue flow that depends on parts/components that conform to a specific specification. This challenge is especially acute for highly regulated life sciences companies that are required to track changes to ingredients used in any pharmaceutical product.
- Explore efforts to provide automated solutions to this process.

2.2.4.3. Risk Tactical Response

Section 2.2.3.2 *Risk Crises Preparation* covered the processes and best practices recommended in order to be ready for a future crisis. This section focuses on the war room processes that need to be mobilized in response to the first potential crisis event reported by suppliers, detected by internal resources, or indicated by an external event monitoring service. It also focuses on the post-mobilization and event resolution postmortem process to assess the response performance, document lessons learned, and fine tune the process as part of a continuous improvement culture.

Critical Success Factors and Best Practices:

> Mobilize war room (based on activation triggers defined in section 2.2.3.2).

- Establish and communicate frequency of meetings, location and/or remote conferencing bridge line joining information.
- Leverage supply chain mapping information to contact suppliers and assess impact.
- Note: This is a critical capability and has specific implications. For example, if a news report indicates a hurricane is heading towards North Taiwan, tracking a list of 300 supplier sites on an outdated spreadsheet is not very useful. Having these sites populated in a mapping system with latitude and longitude is important to visually identify sites in the impact zone. Additionally, capabilities that enable users to circumscribe an area on the map and extract sites, parts, and/or products potentially impacted within a matter of minutes can further minimize time to response.

- Ascertain the revenue impact per part, products and customers potentially impacted to prioritize actions.
- Allocate component part supplies on higher-margin products and adjust production in a cost-efficient way.[33]
- Decisively acquire inventory or capacity for high-impact parts or sub-assemblies and coordinate with Supply Chain Finance on the cost of response and recovery.

> Execute postmortem processes.

- Complete the postmortem evaluation process leveraging the post mortem question checklist provided in section 2.3.3.2.
- Quantify the time and cost of response and recovery. SC Finance is a critical participant. This is because sometimes the team might "save the day" by paying large premiums on freight or expedites, and believe operations were not negatively impacted because customer commitments were not compromised. Supply chain finance may quantify the "real" cost of response in terms of months or quarters of savings that were wiped out in the expedited shipment process. This information may be critical in making a business case for additional investment in SCRP efforts.
- Propose and implement process, solution, and other improvements.
- Reward not just successful response and recovery efforts, but proactive risk avoidance when NOT impacted because of the mitigation undertaken.

2.3. Technology

The systems plan depends obviously on the initial and projected scope and scale of the SCRP organization and project-intensive environments it serves. An appropriate solution can range from an Excel spreadsheet to an enterprise-class cloud system. Gartner identifies four primary enterprise system categories: [34]

- Sourcing due diligence systems conducted in e-sourcing application where supply risk is limited to the evaluation of suppliers as part of the qualification process
- Regulation-specific compliance systems
- ERP, quality modules or proprietary systems that typically track performance by part rather than supplier and have limited functionality (e.g. no ability to integrate third-party data and survey tools)
- Cloud systems

Cloud systems provide an innately suitable architecture for deploying a networked system requiring modern multi-enterprise grid, supplier collaboration/hub, social, and mobile capabilities.

Critical Success Factors and Best Practices:

Regardless of which system approach is taken, the following guidance should apply:

- Define requirements that map to SCRP service offering enablement such as risk intelligence (e.g. network map and supplier repository), risk analysis (e.g. identification, criteria/thresholds/scoring, etc.), and risk monitoring.
- Involve users and partners in the requirements definition to encourage user buy-in and adoption.
- Aim for a single holistic view and "version of supply chain risk intelligence truth." This implies a single system to replace potentially multiple unconnected systems and sources of supply chain data.
- Provide an easy way to report on program metrics that have been identified for each service offering. This includes the ability to easily compose, share, print, and communicate dashboards and reports.
- Make sure that there is a well-thought-out plan to integrate with existing internal systems as necessary such as ERP, quality, sourcing, GRC, regulatory affairs, export management, and PLM systems, as well as external supplier financial data, current and predictive weather and seismic information, commodity price indices, currency feeds, and social media analysis services.
- Ensure there is sufficient emphasis placed on systems training. Solution training should be offered to everyone involved in SCRP processes.
- Be open to cloud-based SCRM offerings from niche born-on-the-web providers (i.e. rather than megasuite vendors such as Oracle and SAP). There is no other practical option today.
- Ensure your technology infrastructure can leverage the latest SaaS, social media,

big data/analytics and mobile technologies.

- Remember that rapid delivery of valued capabilities and aggressive change management are critical to driving adoption.[35]
- Leverage the following checklist as a starting point for developing a requirements specification.

TABLE 9: SYSTEM REQUIREMENTS CHECKLIST

Risk Management Dashboard Analytics Ability to visualize supply chain to identify vulnerabilities and mitigation opportunities
Customized views and analysis of supply network by supplier, sub-contractor, third-party location, part, commodity, product or product family, country, region, custom grouping or geographic selections
Standard risk assessment reports
Easy integration with third-party dashboard and visualization tools
Supplier Network Ability to maintain an accurate map of the supply chain network end-to-end
Complete and accurate n-tier supply chain network mapping and maintenance
Visibility to all relevant upstream and downstream supply chain partner, distributor and customer relationships
Supplier Risk Info Repository Centralization of supplier intelligence in a single repository to facilitate risk mitigation planning, incident response, and supplier collaboration.
Single centralized repository to track additional supply chain initiatives such as conflict minerals compliance, BCP, capacity management, CSR/responsible sourcing, and security (C-TPAT)
Suppliers, locations, and activities tracking
Subcontractors, locations, and activities tracking
Multi-tier (2nd, 3rd, etc.) locations and activities tracking
Alternate sites and recovery times tracking
Third-party emergency contact information tracking
Supplier self-service and multi-enterprise grid functionality
Pro-active Risk Mitigation and Scenario Planning Ability to run risk analytics, quantification models, and "What-If" simulations to proactively identify and mitigate vulnerabilities.

Financial risk score integration in supplier risk analysis, including credit risk, z-score, and debt rating
Location risk score integration in supplier risk analysis, including natural hazards, geopolitical, macroeconomic, and local and site-specific risks
Recovery risk score integration in supplier risk analysis, including recovery time and BCP survey response
Operational risk integration in supplier risk analysis including delivery and lead time performance, quality, cost/flexibility, and capacity metrics
Revenue impact calculation in supply chain risk assessment and analysis
Country risk assessments integration in supplier risk analysis including number of sites and sub-tier dependencies
Proactive assessment of aggregated regional site risks and potential hotspots
Single point of failure analysis by different product groupings to identify single-sourced and difficult-to-replace parts used across multiple product lines
Commodity strategy and risk thresholds settings to calculate and flag parts that are exceptions
Ability to assign commodity manager by part and enable them to open mitigations and track status and approvals
Mitigation resources and budget prioritization based on assessment of high-risk, high-revenue parts/ partners
Supply chain risk mitigation progress, metrics, and target tracking and reporting
"What-If" scenario planning simulations of potential crises situations, results analysis, and pro-active response plan formulation
Ability to view alternative sites, supplier business continuity plans, anticipated recovery times, and expected revenue impact
Identification of parts/suppliers with high risk being designed into new products ("design for resiliency")
Ability to put mitigation strategies in place during design stage
Quarterly business review meetings including supply chain insights and recommendations
Incident Response and Recovery Ability to respond efficiently and effectively to a supply chain incident with virtual Event War Room and "What-If" scenario planning capabilities to minimize customer, financial, and competitive impacts.
24X7 global event monitoring service for real-time event detection and impact analysis
Ability to view the disruption zone and pinpoint supplier sites, products, parts and customers potentially impacted

Ability to identify single-sourced parts potentially impacted, associated recovery times, and inventory on-hand
Ability to quickly secure inventory and identify alternate sites and sources for impacted parts
Workflows to develop pre-determined mitigation strategies and process rules for an automated, coordinated and optimized response
Emergency contact information to quickly verify supplier impact and receive on-going updates
Capability to perform post-event demand-supply matching
Embedded best-practices to ensure proven and consistent crisis response

3. Institutionalization

After the program is launched, the maturation journey begins toward institutionalization. Institutionalization is achieved when supply chain resiliency considerations and best practices are indelibly embedded into the corporate strategy, culture, and operational processes company-wide. Research published in the PwC and MIT PwC and the MIT Forum for Supply Chain Innovation validates that mature risk processes perform operationally and financially better.[36]

A key goal of this phase is for the program to leverage its on-going successes to expand the program along the dimensions defined by the program scope (e.g. more supplier sub-tier visibility, more risk types under management, more supply chain risk initiatives launched such as supplier capacity management, supplier compliance and corporate social responsibility). This includes leveraging the processes and technology platform put in place to map the supplier network, manage a single centralized repository of supplier information, analyze and score risks, monitor and respond to events, and so on.

Here are some key activities.

3.1. Program Monitoring and Management

It is important to operationalize a process for monitoring changes to status, issues, risks, costs, etc. This involves sub-processes for detecting these changes, qualifying and/or quantifying the potential impact, communicating and escalating the impact to relevant stakeholders, and triggering plans of action for resolution or mitigation.

Critical Success Factors and Best Practices:

- Conduct periodic program functional core team reviews to ensure the program is continually aligned and/or consistent with strategic objectives, program planning and operational assumptions, and team needs.
  - Standardize review structure, agenda, attendees, and business process deliverables.
  - Include in agenda:
    - Program scope and objectives review
    - Risk identification review (expect risks to change, evolve, and mutate rapidly)
    - Project planning, delivery, and reporting consistency
    - Task assignment and reporting process and results
    - Issues and challenges
    - Project communication and knowledge/best practice sharing effectiveness
    - Team skills and training needs
    - Resources review (adequacy of people and funding allocated)

- Process maturity progress and metrics
- Continue to define and review standards and processes (e.g. published supplier resilience and risk mitigation standards, regular audits of critical supplier risk factors and resilience scores).

> Conduct quarterly business reviews (QBRs) with critical suppliers to drive improvements in BCP, supplier visibility, and coverage.

> Conduct quarterly business reviews (QBRs) with critical customers to proactively present supply chain resiliency capabilities.

> Conduct new product introduction (NPI) checkpoint meetings to review product resiliency objectives, scorecards and status.

> Conduct regular reviews with executive sponsors and senior leadership (see also 3.2 below).

> Do not underestimate the workload necessary for data maintenance. Standardize and normalize wherever viable; data consistency and quality is essential when expanding beyond Tier-1 partners.[37]

3.2. Working with Governance and Senior Leadership

Maintaining the support of the SCRP governance entity and senior leadership will be critical to long-term survival.

Critical Success Factors and Best Practices:

> Provide a CEO update at least every six months, quarterly CPO updates, and quarterly reviews with functional sponsors (in addition to monthly SC resiliency functional core team meetings and NPI checkpoint meetings to review product resiliency).

> Revalidate with senior leadership with answers to the following:

- Are we providing value?
- Are any changes needed?
- Have we driven our organizations maturity to the next level?
- Can we answer the critical questions?
- Are we addressing the right risks?
- Do we know the current status of all critical suppliers, parts, vulnerabilities, and mitigations?
- Are we managing, escalating, and resolving program issues?
- Does the program staff have the right level of staffing, training, and budget?

> Map intra-company, interdepartmental stakeholders (such as Enterprise Risk Management or Treasury) who might benefit indirectly from the program. For Treasury, which is usually responsible for Contingent Business Interruption (CBI) coverage, there might be an opportunity to leverage the capabilities of the SCRP

efforts to negotiate additional coverage, reduced premiums, lower deductibles, or qualify for difficult to buy insurance.

- Market the program's success. As the program matures it needs to mature in the way that progress and success is shared and communicated. This is a critical need and something that many successful leaders forget to do. Failure to address this diminishes the level of visibility of their work and diminishes the importance of the program and can hamper efforts to advance along the maturity curve. Some strategic initiatives fail to get the visibility and recognition they deserve due to a lack of attention or sophistication in how they market themselves. Marketing the program well internally (e.g. via executive staff meeting roadshows) and externally (by participating in industry forums, speaking engagements, etc.) will serve to further motivate the team (see also 3.4 below), as well as solidify executive support for program growth and expansion.

3.3. Team Motivation and Incentives

Many strategic initiatives fail because team motivation is taken for granted and incentives are not regularly reviewed and re-validated for effectiveness.

Critical Success Factors and Best Practices:

- Include in employee annual targets mitigation targets for high risk components/ suppliers.
- Incentivize supplier management personnel to encourage their suppliers to be more transparent.
- Include in post crisis assessment guidelines for employee recognition not only effective war-room tactics but also risk avoidance and mitigation actions.
- Establish incentives for meeting product, parts and supplier resiliency targets.

3.4. Operationalizing Supply Chain Resiliency and Risk Management

This refers to operational responsibilities for supply chain resiliency and risk management. The role of operations should expand as the program matures. This is because resiliency and risk management best practices become more embedded in operational processes over time. The goal is that fewer and fewer proactive and reactive mitigation exercises are necessary as the program matures. The intelligence that is generated by the risk identification and analysis process is not fed into the risk mitigation/treatment process, but into the business process engineering process so that ultimately they are designed out of the business and operational model.

Critical Success Factors and Best Practices:

- **Supply chain business rules**. This operational practice establishes or configures

business rules to be invoked in an attempt to reduce the likelihood and/or the impact of an identified disruption risk. Business rules may trigger customer priorities, supplier priorities, production routing changes, transportation routing changes, etc. that are designed to minimize the business impact to a supply chain event from either a cost/profit or brand image perspective. Examples of risk management business rules include:

- Sharing orders across multiple suppliers to keep the supplier base "warm"
- Predefined order re-routing procedures in the event of a node failure
- Customer prioritization to allocate scarce resources during an emergency

> **Supply chain network design**. This operational practices relies on a risk evaluation and mitigation at the "network" level -- as opposed to focusing on individual supplier-level vulnerabilities -- in order to guide the design of a resilient and agile supply chain. Node locations, transportation routes, capacity thresholds, locations, number of suppliers and production sites, etc. are all modeled and implemented to drive a more optimal and higher-performing supply chain.

> **"Design for Resiliency."** This process identifies opportunities in the design and development phase to drive resiliency upstream in the product development process by designing out known or potential supply chain risks to product plans such as dependence on a high-risk component or supplier. Key to success include:

- Set risk policies to balance cost savings, time to market, and other targets with resiliency objectives. Example policies may include:
  - Select only components that have multiple sources of supply
  - Select existing compatible/acceptable components rather than requiring an all new design
  - Substitute commodity-grade components with additional testing
  - Do not use of an end of life part, or a part where a last time buy is declared on a new product
  - Avoid use of equipment/tooling which cannot be replaced (because supplier is no longer in business) on new products
  - Use only supplier that meet minimum financial risk standards
- Establish a product level owner (e.g. NPI program manager) to generate a product resiliency scorecard and exceptions. Key scorecard criteria may include:
  - Vulnerable parts, suppliers or locations that a product is dependent on (in terms of location, financial, recovery or operational risks)
  - Product manufacturing and logistic node dependencies
  - Manufacturing redundancy or alternative site readiness/availability
  - Lifecycle of components used in product (e.g. end-of-life)
  - High risk equipment and tooling dependencies for the product (e.g. replace-ability)

- Develop mitigation targets and metrics in order for a product to be approved for release.
- Conduct product release checkpoint meetings and include product scorecard reviews in the agenda in order to make product resiliency scores a mandatory criteria in the product launch gating process.[38]
- Develop a business justification process for exception management that defines approval levels and workflows for exceptions to policies.
- Implement an incentive plan for proactive mitigation execution.

> **Product portfolio rationalization**. Products must reflect realities of the marketplace, which by nature is fragmented and requires multiple tailored approaches. The key is to determine the optimal number of product types and segments. Defining factors include demand volatility, profit margin, supply chain risk and resiliency, and variations in order and manufacturing lead times.[39]

> **Sourcing risk mitigation strategies**. This practice may be appropriate in situations where there is a dependency on a few high-power and/or high-risk suppliers. Options include:

- Multiple sources of supply to minimize single point of failure risks
- Strategic supplier agreements to reserve capacity
- Collaborative Planning, Forecasting and Replenishment (CPFR) to reduce demand surges and supply shortage risks by sharing demand and replenishment data
- Joint product design and delivery to reduce the risk of material non-performance or material shortages[40]

> **Resilience program coordination**. This practice aims to conserve resources and increase risk management effectiveness by taking a collaborative, holistic and risk-sharing approach. It is critical in situations where significant supply chain risks are outside the direct control of the organization and are best mitigated through coordination with partners that can directly act on risks. Tactics include:

- Adopting a common process framework to improve information flow, best-practice sharing, and existing initiative performance, as well as to eliminate ineffective/redundant efforts and coverage gaps
- Establishing a risk management coordination committee to advise and coordinate risk identification and mitigation processes
- Surveying suppliers and conducting recurring meetings to identify critical partners, BCPs and recovery objectives, strategy information, expectations and mutual aid options, and opportunities to mutually further resiliency program maturity levels
- Sharing customer information such as inventory levels, sales volume and demand forecasts to facilitate early detection of supply chain performance risks[41]

> **Contingency business insurance**. Insurance should be leveraged as a core risk

mitigation tool. Insurance provides holistic insurability beyond physical damage coverage to labor strikes, pandemics, regulatory change, civil order and financial failure. Keys to success include:

- Work with insurers to identify requirements for property and casualty insurance. The scope of the coverage should include non-physical damage.
- Document current insurance coverage, deductibles and premiums. Identify if this is adequate for supply chain dependencies in the sub-tier supply chain (named versus unnamed coverage).
- Provide supply chain mapping and visibility data to insurers.
- Annually present supply chain risk program and mitigation processes and methodology to insurer.
- Leverage SC Mapping data for determining what to insure and how much coverage to buy.
- Note that while insurance can mitigate a negative financial impact it cannot neutralize negative impact to brand or shareholder value.

> **Price management sensitivity analysis**. This can be used as a means of reducing risk in demand management and shaping efforts.

3.5. Positioning the Program for Future Success

The following tools, concepts, and trends may be critical to institutionalization of SCRPs. Reflection on their role may be critical in keeping the SCRP relevant and successful well into the future.

Critical Success Factors and Best Practices:

> **Consider adopting a maturity model**. Maturity models can provide a practical next step as well as a guiding light toward an aspirational yet achievable SCRP vision. Excellent maturity models have been developed by Gartner, KPMG, and PwC.

> **Prepare to have less and not more control**. With the unabated march towards a more specialized and connected world, supply chain practitioners will increasingly need to prepare for a world where risk is even more diffused and even less directly controlled. As a result, core competencies in supply chain partner collaboration, risk sharing, and network-performance optimization will be critical for business survival.

> **Deploy a Center of Excellence (CoE)**. Deploying a CoE usually involves establishing a multi-disciplinary team to focus on standardizing business processes and providing continuing education for key managers. CoEs are a key sign of successful program institutionalization if they are hosted at high levels in the organization. However, if the CoE is buried within the organization, it will lack the required independence to make the tough calls and defy the status quo.[42]

> **Live or die by your analytics**. Plan for a future driven by analytics to sift through

the increasing preponderance of structured and unstructured data. For example, supply chains will become an integral part of the Internet of Things (IoT) as products, parts, and shipments/containers with sensors communicate structured data about their location, surrounding environment, and other attributes. Unstructured data will flow from external sources including social media used to measure customer sentiments and trends, as well as to sense and report on local disruption events.[43]

- **Plan for security issues to explode**. Supply chains of the future will have to factor IP and patent protection risk into sourcing and trade decisions. IP theft and piracy will continue to grow. Western notions of business ethics in countries like China are essentially irrelevant.[44]
- **Join or take a leadership role in building a SCRM professional community**. The institutionalization process within your organization can be facilitated by institutionalization of resiliency across the industry. Professional communities such as the Global Supply Chain Resiliency Council can accelerate the process by sharing best practices, cross-pollinating ideas, and promoting individual and company success stories that can bolster the business case or accelerate investments in SCRPs.

Conclusion

If you have been tasked with forming and managing a SCRP, the steps outlined in this white paper provide a starting point. Once you have followed these steps and have a detailed description of how you'll launch and develop your SCRP organization, you move on to communicating this plan to key stakeholders and, of course, managing your plan in action.

Acknowledgements

While Resilinc is the primary source of the ideas, opinions, and content contained in this document, our thinking has been shaped by countless interactions with industry practitioners and research analysts either through direct dialogue, published works or other content shared in the public domain. Their ideas are infused throughout this guide. In that light, Resilinc would like to especially acknowledge the contributions of ChainLink Research, Gartner, the Supply Chain Leadership Council (SCLC), ANSI/ASIS, and Cisco.

Citation Number	Source
[1][28][29][33][36]	PwC and MIT PwC and the MIT Forum for Supply Chain Innovation, 2015
[2][12][16][24]	"Managing Risk in the Global Supply Chain" The University of Tennessee, 2014
[3][30]	Noha Tohamy, Gartner 2012; 2008
[4][5][9][11][14][15][20][25][41][42][43][44]	"Supply Chain Management: A Compilation of Best /Practices" ANSI/ASIS, 2011; 2014
[6][18][19][39][40]	"Managing Risk in Your Organization with the SCOR Methodology" The SC Council Risk Research Team, 2008
[7][37]	Christian Titze, Gartner, 2015
[8][13][17][21]	Gary Lynch, 2014; 2011
[10][22][23][34]	"Strategic Road Map for Supply Risk Solution Deployment" Deborah Wilson, Ray Barger, Gartner 2014
[26]	Mark Hillman, Gartner, 2007
[27]	ISO Guide 73:2009
[31]	"Four Best Practices for Minimizing Global Supplier Risk" Paul Mandell, Supply Chain Management Review, 2014
[32]	Tim Payne, Gartner, 2009
[38]	"Supply Chain Risk Management at Cisco" Embedding End-to-End Resiliency in the Supply Chain", Cisco, 2012

Disclaimer

© 2015 Global Supply Chain Resiliency Council and Resilinc, Inc. The information contained in this publication represents the opinions of Resilinc or has been obtained or inferred from sources believed to be reliable. Resilinc disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This publication consists of the opinions of Resilinc's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Although Resilinc research may include a discussion of related legal issues, Resilinc does not provide legal advice or services and its research should not be construed or used as such.