# Supply Chain Risk Management: A Compilation of Best Practices

*August 2011*

SCRLC

SUPPLY CHAIN RISK LEADERSHIP COUNCIL

# 1. Executive Summary: The Need for Supply-Chain Risk Management

Modern enterprises increasingly find themselves relying on others for their success. Historically, enterprises have spent less than a third of their budgets on purchased goods and services, having relied on internal sources for these. Today, many enterprises spend most of their budget on purchased goods and services. This is in large part because of the advantages enterprises have found in strategies such as globalization, outsourcing, supply-base rationalization, just-in-time deliveries, and lean inventories. In addition, many companies have consolidated operations both internally and externally to achieve economies of scale.

While globalization, extended supply chains, and supplier consolidation offer many benefits in efficiency and effectiveness, they can also make supply chains more brittle and can increase risks of supply-chain disruption. Historic and recent events have proven the need to identify and mitigate such risks. The March 2011 Tohoku earthquake and subsequent tsunami in Japan showed how one event can disrupt many elements of global supply chains, including supply, distribution, and communications (Lee and Pierson, 2011). In extreme cases, a single event at one location can severely damage an enterprise or even cause it to leave an industry.

Effective supply-chain risk management (SCRM) is essential to a successful business. It is also a competence and capability many enterprises have yet to develop. In some areas, both problems and practices are well defined. In others, problems are defined, but practices are developing. In still other areas, both the definition of the problems and the practices needed to address them are developing. In sum, SCRM is an evolving field.

In this document, the Supply Chain Risk Leadership Council (SCRLC), a cross-industry council including supply-chain organizations from more than two dozen world-class manufacturing and services firms and academic institutions, outlines an approach to SCRM. This document provides a framework for collecting, developing, and implementing best practices for SCRM. It focuses on

- Identifying internal and external environments
- Risk identification and assessment
- Risk treatment
- Continual monitoring and review of risks and their treatment.

This document is meant to be a practitioner's guide to SCRM and associated processes. Approaches for identifying, evaluating, treating, and monitoring supply chain risk will differ across individual enterprises depending on their industry, the nature of their extended supply chains, and their tolerance for risk (or risk appetite). Therefore, rather than prescribing a specific approach to SCRM, this document notes some guidelines and possible approaches an organization may wish to consider, including examples of tools other organizations have used. Specific enterprises will adapt the concepts included in this document to fit their unique characteristics and expand the depth and breadth of the processes to meet the requirements of their organizations.

This document excludes risks such as those to brand reputation or intellectual property which exist outside the supply chain. It seeks to foster the development of best SCRM practices for application in industrial settings rather than provide a regulatory framework.

This is a working document. Its contents reflect a collection of best-practice inputs from SCRLC members. The inputs on supply-chain risk management are, to our knowledge, unique, though based in part on previous works regarding supply-chain risk more generally. The problems of SCRM and the means to address them will continue to change. As they change, we hope to both update this document and to issue additional publications detailing evolving areas. This document serves as a baseline for both helping enterprises assess and address supply-chain risks and for documenting evolving practices. We seek collaboration to promote these practices for supply-chain resiliency.

## *About the SCRLC*

The SCRLC (http://www.scrlc.com) is a cross-industry organization including world-class manufacturing and services supply-chain organizations and academic institutions that work together to develop and share best practices in supply-chain risk management. Its mission is to create supply-chain risk management standards, processes, capabilities, and metrics that reflect current best practices and can be widely adopted.

## 2. SCRM: An Overview

The SCRLC defines "supply-chain risk" as the likelihood and consequence of events at any point in the end-to-end supply chain, from sources of raw materials to end use of customers, and "supply-chain risk management" as the coordination of activities to direct and control an enterprise's end-to-end supply chain with regard to supply-chain risks.

Supply-chain risk management integrates several previous or ongoing initiatives, including those for business continuity and supply-chain security. Supply-chain security-management systems seek to resist "intentional, unauthorized act(s) designed to cause harm or damage to, or by, the supply chain" (ISO 28000:2007). SCRM goes beyond this by not only seeking to address such acts but also to promote business continuity and to mitigate any disruptions, that is, events that interrupt normal business, activities, operations, or processes (ASIS International, 2007; ASIS International and BSI, 2010). Such events may not only be intentional acts such as sabotage but also unintentional acts such as a hurricane. They may be both events anticipated, such as political unrest, or unanticipated, such as an earthquake.

### *Risk Management Process Overview*

In this document, we provide an approach to risk management. Our process, based on ISO 31000, covers elements of risk identification, risk assessment, and risk treatment (Figure 2.1). ISO 31000 is a key building block to our approach; while adapting it to our own purposes, we recognize the need to avoid replicating standards documents but rather to strive for practices that cover security, crisis, continuity, and recovery requirements enterprises may have.

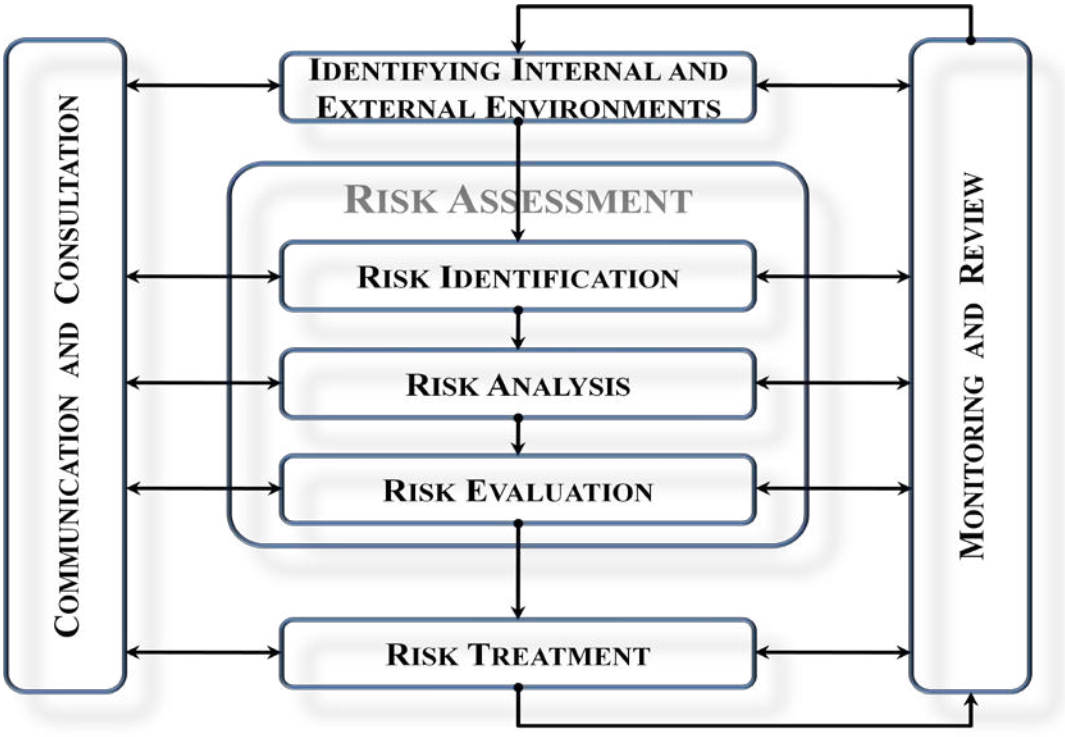



**Figure 2.1: Risk Management Process**

The process begins with *identifying internal and external environments*. Enterprises may inadvertently overlook internal risks. These may include those posed by a rogue employee, as well as those posed by inadequate policies, strategies, or

organizational structures. The external environment in which an enterprise, and its suppliers, must work will also pose differing risks. For example, some suppliers will face meteorological risks, while others, because of their distance, may have greater transportation risks. Mapping its supply chain can help an enterprise identify the risks it faces and how best to prioritize and address them. To prioritize and address risks, firms will need to identify criteria for determining what may pose a risk to its operations. One potential starting point is the supply chains for the products most affecting firm profitability.

Once a firm understands how to identify risks, it may undertake *risk identification and assessment,* which includes risk identification, risk analysis, and risk evaluation. Risk identification may entail using a list of common risks including external risks such as natural disasters, accidents, sabotage, or labor uncertainty; supplier risks such as production problems, financial issues, or subcontractor problems; distribution risks such as cargo damage, warehouse inadequacies, or supply pipeline constrictions; and internal risks such as personnel availability or facility unavailability. (See Appendix 2.1 for a list of sample risks by category.) Such process will also involve prioritizing risks by the threat (as measured by likelihood and consequence) they can pose to a firm's operations.

Once a firm has identified and prioritized the risks that it faces, it can devise *risk treatment* plans. This includes measures to protect the supply chain from risks, plans to respond to events that these risks may cause, and plans to continue operations in the face of disruptions and fully recovering from them. This may also involve determining ways to measure risks and the effectiveness of plans to limit them or to respond to disruptions.

Enterprises must also undertake continual communication and consultation as well as *monitoring and review* throughout this process. Monitoring and review entails not only evaluating the effects of risk treatment but also maintaining the plan and responding to changes in suppliers, processes, and regulation affecting elements of the supply chain. It also entails continually identifying opportunities for improvement.

## *Principles of SCRM*

Efforts to implement SCRM must address four principles: leadership, governance, change management, and the development of a business case.

Leadership support and guidance is essential to any successful SCRM program. An integrated and engaged leadership team can not only help identify risks well before they cause disruptions but also provide a quick and thorough response to any incidents that might occur. Ultimately, leadership, reporting and ownership of supply-chain risk should rest with senior management.

An effective SCRM team should include leaders from functions such as

- Business continuity
- Engineering and design
- Enterprise risk management
- Finance
- Governance
- Import/export compliance
- Logistics

- Manufacturing
- Procurement
- Quality
- Security
- Supplier management.

Differing functions should have representation on both the executive steering team and the implementation team.

It is most effective to have an executive sponsor who is skilled in the area in which the firm faces the greatest risk. For example, if timely transportation of components is the most vital function for a firm and the one where it may face the greatest risks, then it may wish to have a logistics executive be the executive sponsor of the SCRM team. Corporate culture, including the area that a company most wishes to emphasize to build its reputation, may also determine executive sponsorship for the SCRM team. For example, a manufacturing firm may choose to have a manufacturing executive be the executive sponsor of the SCRM team, regardless of the greatest supply-chain risks. One leading firm rolls up risks to the chief information officer, to whom responsibility for supply-chain risks was originally given. Another has a vice president of risk manager. A leading insurance provider has its chief operating officer assume ultimate responsibility for risk management. In many mid-sized companies, the chief financial officer may have ultimate responsibility for risk management.

The team should ensure that risk-management processes are embedded into business-function processes so as to ensure proper communication and collaboration on events. Regular (e.g., monthly) meetings of the implementation team can help ensure proper communication, as can less frequent but still regular (e.g., quarterly) meetings of the executive steering team. One leading firm briefs its executive board quarterly on supply-chain risks and what is being done to address them.

Ideally, a firm will have detailed governance procedures for a continuing supply-chain risk management team, including those on meeting structure, attendees, standard agenda items, and business-process deliverables. Typical agenda items might include process maturity, metrics, compliance, and audits; a review of risks and how the firm is addressing them, and sharing of knowledge and best practices. Supply-chain risk management teams should use inputs from lower-level working groups and process users to influence decisions of higher-level executives in determining appropriate resources and priorities for their efforts (Figure 2.2).

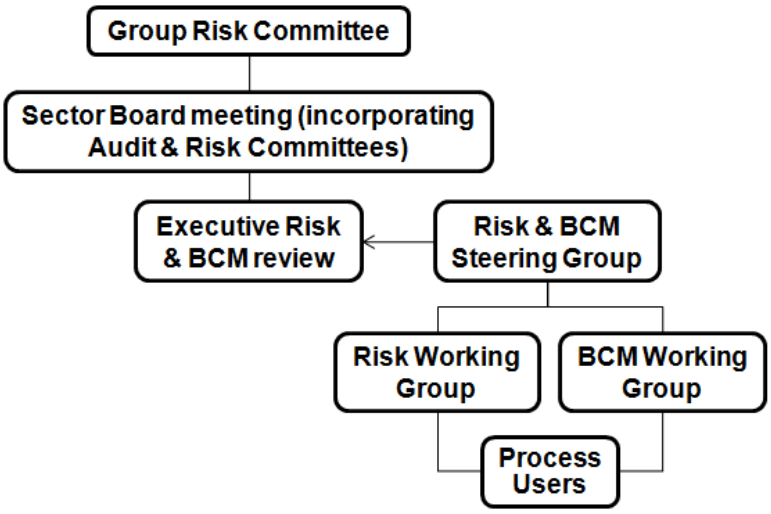



**Figure 2.2: Notional Risk Management Governance Structure**

Establishing or improving SCRM in most enterprises represents a major change. Consequently, those implementing SCRM will need to pay particular attention to the tenets of successful change management. These include a compelling case for change, unwavering senior leadership support, and a clear vision of the future with the change. They also include development of an action plan for implementation as well as ongoing monitoring and refinement to reflect lessons learned. Lastly, they require sustained communication with key stakeholders through the change, proactive education and training so that personnel have the skills to execute the change, incentives aligned with the desired outcomes of the change, and adequate resources to successfully manage and implement the change. Because resistance is natural and to be expected with a major change, those implementing SCRM also need to pay attention to the psychological and emotional aspects of the change. Linking it to other corporate supply chain objectives such as corporate social responsibility and carbon footprints can also be useful.

The business case for SCRM has several components. SCRM can offer cost savings by protecting against sales and market-share loss and rebuilding costs. SCRM can also offer enterprises a competitive advantage if it enables an enterprise to recover faster than its competitors. Disruptions carry costs as do workers who must log additional hours to compensate for shortfalls caused by disruptions and warehouses needed to store items needing key parts for completion. Identifying these cost savings can help justify SCRM investments, especially if these investments can otherwise help firms make the most of their resources. SCRM can also offer intangible benefits. These include avoiding damage to reputation or brand that may accompany a supply-chain disruption as well as breaking down organizational silos, which is not only necessary for SCRM but can also help enterprises in other initiatives.

As an example, a leading firm with an established, strong SCRM program, uses a metric titled "Time to Recover (TTR)" to reflect and measure the business case for investing in their SCRM program. Product output and revenue are directly impacted under multiple risk scenarios. By identifying, assessing, and mitigating these risks, this firm targets specific reductions in the TTR for their business. Forecasting TTR with and without risk mitigation shows the effects, in revenue, of SCRM. Indeed, this firm claims a focus on TTR metrics in its SCRM helped it save millions it would have lost in subsequent events.

We turn next to how firms may begin identifying their internal and external environments.

## 3. Identifying Internal and External Environments

Risks exist at discrete levels and entities within an organization. Manufacturing risks exist at manufacturing sites. Supplier risks exist at supplier sites (including those of sub-tier suppliers). Distribution risks exist at suppliers and in upstream and downstream transportation and logistics systems (Figure 3.1). Legislative, compliance, intellectual property, and regulatory risks exist at the country or regional level for multinational enterprises. Finally, strategic risks exist at the business-unit or corporate level.

Credit: E. V. Leyendecker, U.S. Geological Survey. Photo is of Interstate 880 in Oakland, California after Loma Prieta earthquake of 1989,

***Figure 3.1: Earthquakes Can Pose Risks to Transportation and Security***

Enterprises must identify, own, and manage risks at the level they exist. Enterprises must also aggregate and report risks across the organization and vertically through business reporting structures. Enterprises should give risks that exist within multiple entities common, coordinated treatments.

When lower-level risks are identified at higher levels of the enterprise but not owned at those levels, it may be necessary to implement governance controls to assure that risks are managed throughout the enterprise and supply chain. Such risks may arise when franchises make for local consumption a final product whose performance will affect reputation of a more widely used corporate brand. They may also arise when performance of a lower-tier supplier disproportionately affects the reputation of a large manufacturer as has happened, for example, in the use of lead paint by lower-tier suppliers on toys ultimately assembled and sold by large firms with strong brand-name recognition. Governance controls to manage such risks may include corporate leadership setting policies, procedures, and standards for lower levels to follow, with governance supported by compliance activities such as auditing. Enterprises cannot tell

franchises how to operate their facilities, but, as they do with ensuring compliance with corporate social responsibility practices, they can provide guidelines.

The presence of differing risks at differing levels of an enterprise underscores the importance of defining the context within which a risk-management program is implemented. This includes suppliers, manufacturing, logistics (e.g., warehousing and distribution), customers, and other elements that can affect the supply chain. These elements will vary by industry, as will the efforts an organization can make to address them. For example, a manufacturing plant may have more control over assembly risks than a higher-level business unit, while a business unit may be better able to address supply-chain risks posed by legislative and regulatory issues and to coordinate efforts to mitigate some procurement risks.

A key decision in developing an SCRM program is the scope of the supply chain to include. Enterprises may initially focus on Tier 1 suppliers, or even prioritize among Tier 1 suppliers. In most cases, the scope should include all tier 1 suppliers and customers. In determining how much of the supply chain to include beyond the first tier, managers may wish to characterize inputs by the number of suppliers and number of customers. For example, at one extreme, for commodities with a large number of suppliers, it is likely not necessary to go beyond the first tier in considering supply-chain risks. At another extreme, for materials with few suppliers or only one, it is necessary to consider risks among second-tier suppliers. Between these two extremes firms need to assess how critical a particular component is or how easily a supplier can be replaced and, if necessary, consider supply risks in the second tier for critical components or suppliers.

By repeating this process for increasing numbers of tiers of suppliers and customers, enterprises can capture the portions of the supply chain that have the greatest risks to operations. Such an approach is only a guideline; specific knowledge of an organization and its industry is necessary to guide decisions.

Mapping supply-chain processes can help enterprises understand the potential risks that exist as well as the organizations involved. Figure 3.2 presents a notional map. Upstream, it originates with raw materials, parts, assemblies, and packaging going to suppliers, some of which may flow directly to the final production or assembly point as well. Distribution systems, including trucks, trains, ships, and aircraft, move components from suppliers to the inventory of manufacturers, as well as from manufacturers to the inventory of customers. Several elements are common to all these elements and can be the source of risks throughout the supply chain. These include infrastructure such as buildings and equipment, utilities whether “raw” (e.g., water) or “converted” (e.g., refrigeration), process functions such as production planning or sales and operation planning (S&OP), and personnel, including salaried and hourly workers as well as temporary workers and contractors. Not all these nodes will have risks for all operations, but all should be considered.

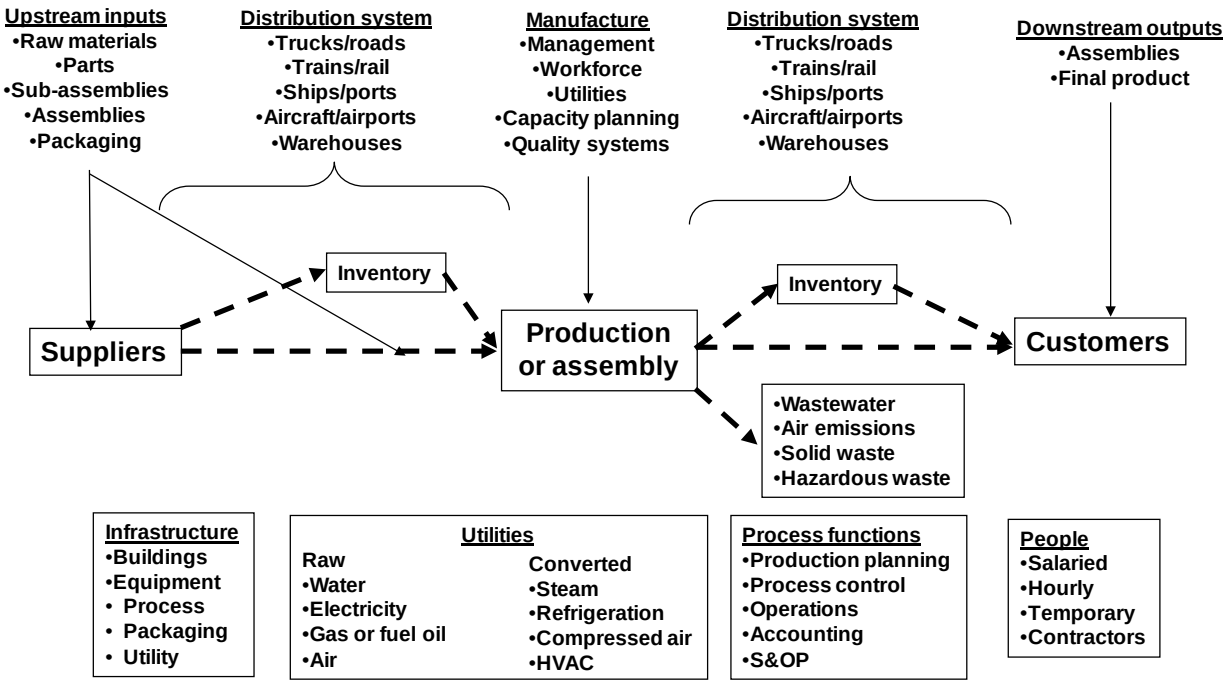



***Figure 3.2: Notional Supply-Chain Process Flows***

Information flows should also be documented. Information can flow both upstream and downstream. In particular, information flows on downstream conditions can help upstream processes provide the correct quantity and quality of materials needed.

Organizations should map the supply-chain elements for which they are directly responsible and that they control. They should also extend the supply-chain map at least one tier up and one tier down, considering direct suppliers and direct customers including transportation and information links for them.

Firms may use several criteria to identify risks (Moore, Grammich, and Bickel, 2007). Pareto analysis, also known as A-B-C analysis, can help firms identify the proportion of goods and suppliers on which it is most dependent in terms of profitability or criticality, and hence the goods and suppliers that can pose the most risk to the supply chain. More sophisticated portfolio analysis can help firms identify goods by both their value and the vulnerability of supply, and lead firms to focus their SCRM first on strategic or critical goods of high value and high supply vulnerability. These may include scarce or high-value items, major assemblies, or unique parts, which may have natural scarcity, few suppliers, and difficult specifications. We next examine how firms can identify and assess risks.

# 4. Risk Assessment Process

A solid risk management program, from initial deployment to sustainable operation, includes a robust and ongoing risk identification and assessment process. That is, it includes a risk-assessment process that is able to evaluate a wide variety of risks over time.

The risk-assessment process should distinguish between risks that should be included in the risk-management process and those that should not. 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 risk-management process. Characteristics that can cause abnormal variations, that is, those which the supply chain cannot flex and respond to, should be included.

## *Risk Identification*

Developing an initial risk register, which is a one-time effort, is necessary to identify baseline risks. Too many organizations start a risk management program without knowing what threats the organization faces, or what consequence a disruption would have. As a result, they focus too much protecting against the wrong threats or too little protecting against threats that matter. Worse, they may fail to anticipate important threats, or fail to recognize the consequence an apparently minor threat may have.

Risk identification might begin with brainstorming sessions, previous risk assessments, surveys, or still other efforts to identify and list potential risks within supply-chain processes. Reference works that can help with identifying risks include those from the British Standards Institution (BS 31100:2008), which offers a code of practice for risk management, and from the ISO (ISO 31010:2009), which offers a compendium of risk assessment techniques.

A business-impact analysis can help a firm evaluate the threats a firm might face and their consequences. Such analysis might start with a "worst-case" scenario focusing on the business process that are most critical to recover and how they might be recovered remotely. A business-impact analysis should identify critical business functions and assign a level of importance to each function based on the operational or financial consequence. It should also set recovery-time objectives and the resources required for these.

Table 4.1 presents examples of threats an organization may wish to consider for mitigation. Appendix 2.1 (referenced earlier) presents a longer but not exhaustive list. Note that risks can overlap categories.

### *Table 4.1: Potential Risks to an Organization and Its Supply Chain*

*External, End-to-End Risks*

- Natural disasters
- Sabotage, terrorism, crime, war
- Labor unavailability
- Lawsuits
- Accidents
- Political uncertainty
- Market challenges
- Technological trends

*Supplier risks*

- Physical and regulatory risks
- Financial losses and premiums
- Upstream supply risks
- Production problems
- Management risks

*Distribution Risks*

- Infrastructure unavailability
- Lack of capacity

- Labor unavailability
- Warehouse inadequacies
- Long, multi-party supply pipelines
- Cargo damage or theft
- IT system inadequacies or failure

*Internal Enterprise Risks*

- Operational
- Demand variability
- Design uncertainty
- Financial uncertainty
- Testing unavailability
- Supplier relationship management
- Political uncertainty
- Personnel availability
- Planning failures
- Facility unavailability
- Enterprise underperformance

To identify risks, firms may also wish to consider

- Number and location of suppliers. For example, are there suppliers in countries with social unrest (Figure 4.1), terrorist or drug activity, or high levels of corruption?
- Number and origin of shipments. For example, have increased quantities or values of shipments posed additional risks?
- Contractual terms defining responsibility for shipping. For example, firms may specify security controls and procedures for their suppliers. (Appendix 4.1 provides sample contractual terms and conditions for supply-chain security.)
- Modes of transport and routes for shipments. For example, firms may ask their suppliers follow certified security procedures for ocean-container or truck-trailer shipments.
- Other logistics providers or partners involved in the supply chain (e.g., packaging companies, warehousing, trucking companies, freight forwarders, air or ocean carriers), who handle shipments. For example, firms may that logistics providers meet all certification standards form an official supply-chain security program.
-

Credit: Photo of Paris demonstrations and riots following May 2007 election of Nicolas Sarkozy by Mikael Marguerie,

***Figure 4.1: Unrest Can Strike Anywhere at Unpredictable Times***

Not all possible risks, of course, will threaten organizations equally. Locations are not, for example, equally at risk for meteorological threats to their operations. Organizations may wish to use operational exercises to determine if they have identified all plausible threats for a given location. They may also wish to use such exercises to analyze risks and evaluate their responses to them.

The initial risk register, even if including all identified risks for mapped processes, will likely not cover all risks, or even all significant risks to the supply chain. It is a starting point to identify relevant supply-chain risks. Once the baseline risks

are identified, the organization should periodically review the status of risks in the risk register, incorporating new risks as they develop and eliminating risks that are no longer relevant.

## *Risk Analysis*

The risk analysis process should estimate the likelihood and consequence of risks facing a firm and accordingly prioritize them for ultimate treatment. To begin, firms may choose to rank risk events based on a qualitative overall risk level. Such a simplistic approach should only be used for the initial risk register, but provides an easy way to quickly prioritize perceived risks and select those that should receive priority attention.

Once an enterprise has identified its top risks, it may use more sophisticated methods, such as the bow-tie method, to fully understand the nature of the risk and to rate the likelihood and consequence of inherent risk (i.e., risk in the absence of any treatment) and residual risk (i.e., level of risk remaining after treatment). The bow-tie risk analysis method is a form of cause and consequence analysis—the two dimensions of risk events—and it clearly ties treatment actions against each dimension of a risk event. Figure 4.2 shows an example of the bow-tie method.

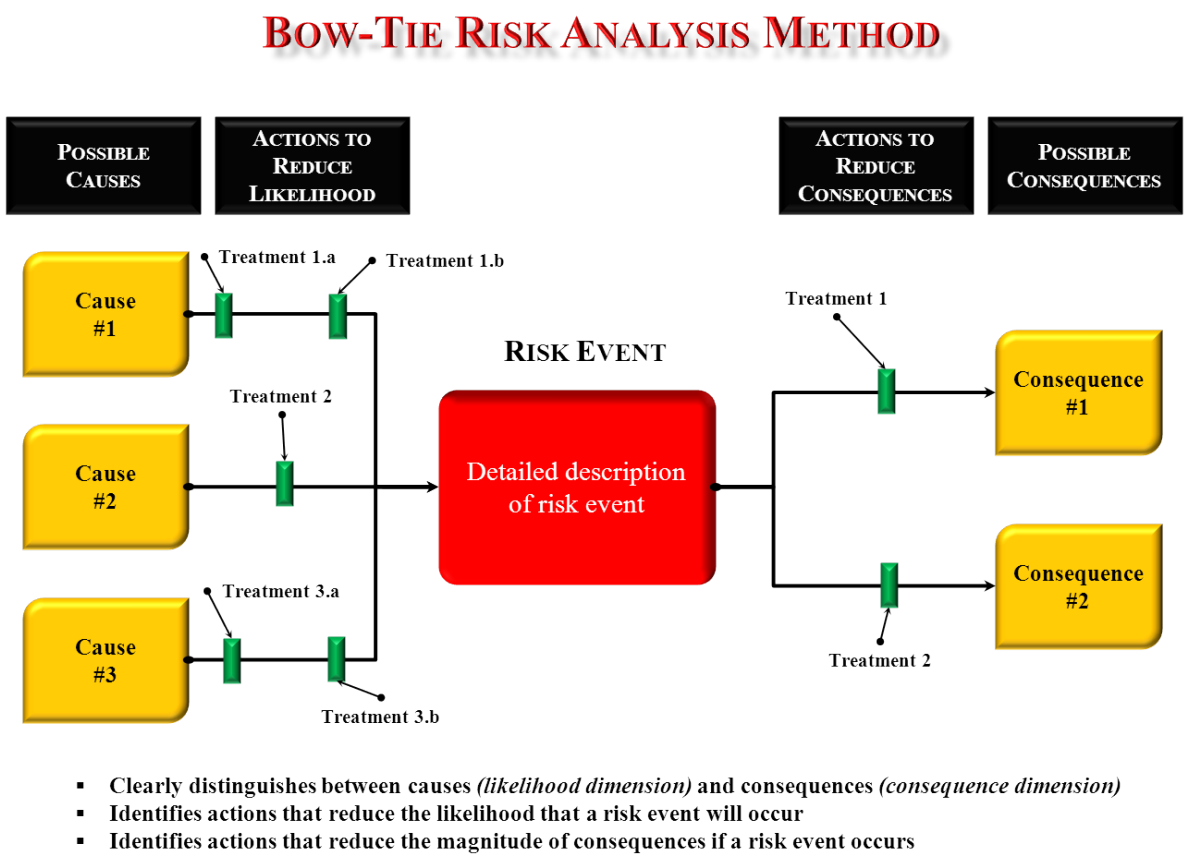



***Figure 4.2: Bow-Tie Method for Linking Treatment to Cause and Consequence***

For example, a manufacturer may face risk of shutdown resulting from an earthquake, a fire, a flood, failure of a key supplier, or temporary loss of workers due to an infectious disease outbreak (Figure 4.3). In analyzing its risks, it may wish to determine the likelihood of each of these events. Likewise, it may wish to rate the consequences of such events. Five-point scales of likelihood (ranging, for example, from less than 5 percent for the least probable to more than 90 percent for the most probable) and consequence (ranging, for example, from less than 2 percent of gross revenue or 4

percent of net revenue for the least consequential to more than 20 percent of gross revenue or 40 percent of net revenue for the most consequential) may suffice for this. Inherent and residual risks may then be calculated and compared by combining likelihood and consequence ratings before and after treatment.

Credit: Photo of 2009 fire and explosion at Caribbean Petroleum Corporation refinery near San Juan, Puerto Rico from U.S. Chemical Safety and Hazard Investigation Board,

***Figure 4.3: Fires Can Shut Facilities for Varying Lengths of Time***

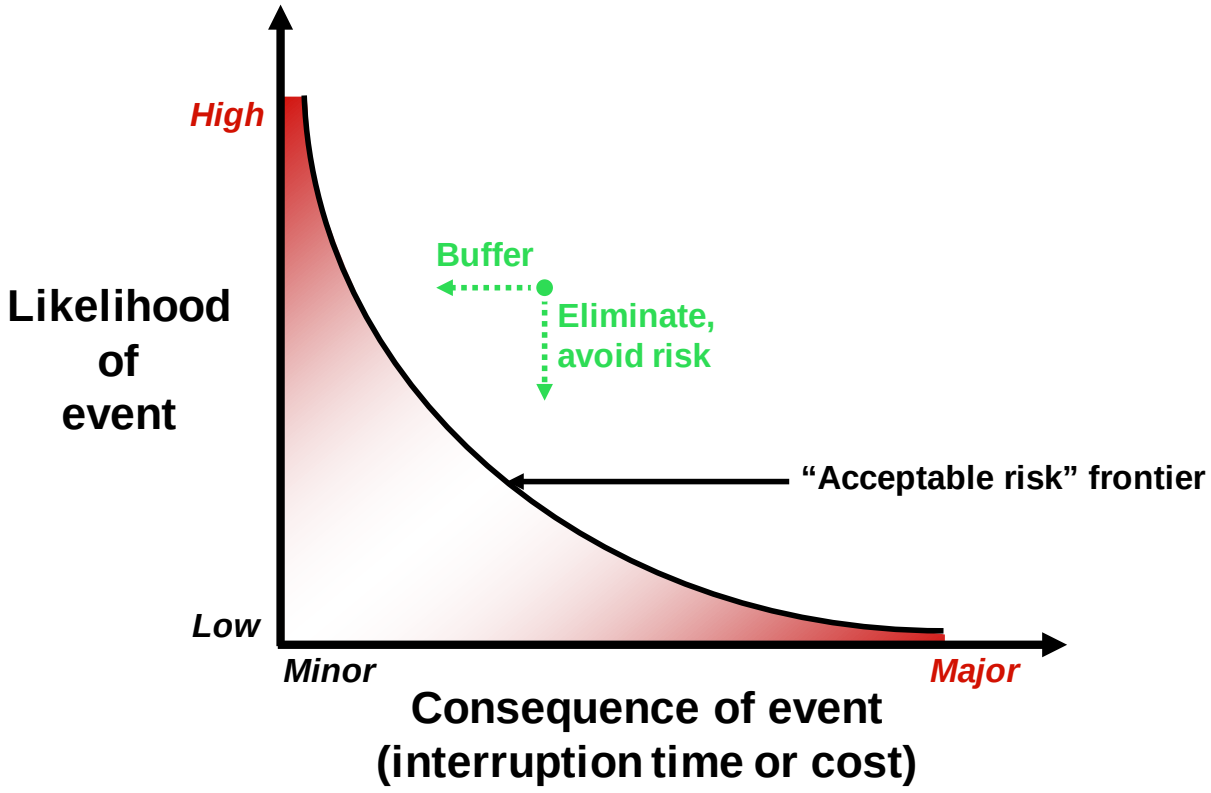
## *Risk Evaluation*

Enterprises may use their ratings of the likelihood and consequence of risks before and after treatment to evaluate residual risk levels against acceptable risk levels, that is, their risk tolerance. If the likelihood and consequence of residual risks is found to be greater than their risk tolerance, then enterprises need to devise further risk treatments to reduce the level of residual risk.

Acceptable risk levels will be unique to each organization and supply chain. They may vary by commodity, product, or service, as well as over time. Different risk-tolerance levels may be set for different levels of the organization. While generally tied to financial impact, through which risks may best be understood and compared, risks may also be tied to other corporate assets such as reputation. One leading firm even considers the consequence of potential risks by impact to stock price.

One way an organization may wish to assess its risk tolerance is through a risk "frontier" graph, plotting the likelihood of events by their consequence (Figure 4.4). Enterprises may find some risks to be of such low likelihood or to have such limited consequence that they do not warrant any further treatment or consideration. Those of greater likelihood or consequence enterprises may wish to reduce through various buffering (e.g., use of multiple suppliers or safety stocks)

or other mechanisms of risk avoidance or elimination. Such mechanisms may seek to reduce the likelihood, duration, or consequence of a risk event.




SOURCE: Zsidisin, Ragatz, and Melnyk, 2003

*Figure 4.4: Notional Risk "Frontier"*

Another means of evaluating risk is to use a "heat-map" showing risk-events on a matrix defining likelihood and consequence levels. This technique allows managers to easily see the relative likelihood and consequence of differing risks. To use this method effectively it is critical to have well-defined and consistently used criteria for the different likelihood and consequence levels. Figure 4.5 shows a heat-map illustrating the concept.

| LIKELIHOOD | insignificant | minor | moderate | major | critical |
|---|---|---|---|---|---|
| almost certain | Moderate | Major | Critical | Critical | Critical |
| likely | Moderate | Major | Major | Critical | Critical |
| possible | Moderate | Moderate | Major | Major | Critical |
| unlikely | Minor | Moderate | Moderate | Major | Critical |
| rare | Minor | Minor | Moderate | Moderate | Major |

CONSEQUENCE

***Figure 4.5: "Heat" Map Showing How Firms May Wish to Prioritize Risks by Likelihood and Consequence***

We turn next to how an enterprise, having prioritized its risks, may seek to address them.

# 5. Risk Treatment

Once an enterprise understands its supply chain and analyzed its potential risks, it can implement an effective supply-chain risk management program with its partners, that is, its suppliers, carriers, and logistics providers. Such a program should have at least three elements: protecting the supply chain, responding to events, and continuing business operations while recovering from events. We discuss each of these below.

## *Protecting and Securing the Supply Chain*

An effective supply-chain risk management program must ensure that an enterprise and its partners implement appropriate measures to fully secure goods and their components from the point of origin to final destination. Supply chain security is essential from two perspectives. First, firms need to prevent loss from theft or damage. Second, they need to prevent unauthorized intrusion into shipments that could enable insertion of contraband (drugs, weapons, bombs, human trafficking, counterfeit goods, etc), loss of intellectual property or technology contained in the shipments, and tampering (insertion of harmful elements such as poisons or "Trojan horses" in computing goods).

Effective supply chain security and protection includes basic standards for physical security, access controls, personnel security, education and training, procedural security, information-technology (IT) security, business-partner security, and conveyance security from the point of origin to final destination within your supply chain.

Enterprises and their partners may assess their effectiveness with these measures through self-evaluation (Appendix 5.1). We discuss some benchmark standards for each of these criteria below. Firms may wish to adapt or emphasize these in unique ways to reflect the unique risks they must address. For example, pharmaceutical and electronic goods companies may have high value shipments that are at far more risk for theft than other commodities.

*Physical security*. Suppliers, shippers, and logistics partners should have physical-security deterrents to prevent unauthorized access to their facilities and all cargo shipments. Such features may include perimeter fencing, controlled entry and exit points, guards or access controls, parking controls, locking devices and key controls, adequate lighting, and alarm systems and video-surveillance cameras.

*Access controls*. Access controls must prevent unauthorized entry to facilities, maintain control of employees and visitors, and protect firm assets. They should include the positive identification of all employees, visitors, and vendors at all points of entry and use of badges for employees and visitors. Firms should have in place procedures to identify, challenge, and address unauthorized persons.

*Personnel security*. Enterprises and their partners should screen prospective employees (in ways consistent with local regulations) and verify employment application information prior to employment. This can include background checks on educational and employment background and possible criminal records, with periodic subsequent checks performed for cause or sensitivity of an employee's position. Firms and their partners should also have procedures in place to remove badges, uniforms, and facility and IT-system access for terminated employees.

*Education and training.* Firms and their partners should establish and maintain a security-training program to educate and build employee awareness of proper security procedures. Best practices include training on the threat posed by criminals, terrorists, and contraband smugglers at each point in the supply chain as well as on ethical conduct and the avoidance of corruption, fraud, and exploitation.
Enterprises and their partners may especially wish to ensure employees in shipping and receiving understand proper

supply-chain security measures. Education and training should also include documented procedure for employees to report security incidents or suspicious behavior.

*Procedural security.* As noted above, firms and their partners should establish, document, and communicate procedural security measures to employees. Such documentation may include a security manual, published policy, or an employee handbook. Documentation should include procedures for issuing accessing devices, identifying and challenging unauthorized or unidentified persons, removing access for terminated employees, IT security and standards, reporting of security incidents or suspicious behavior, inspection of containers before packing, and managing access and security to shipping containers. For shipping, such procedures should include security for shipment documentation, shipping and receiving, and packaging.

*IT security*. IT security measures should ensure automated systems are protected from unauthorized access and that information related to shipment routing and timing is protected. This should include password protection (including periodic changing of passwords) and accountability (including a system to identify any improper access or alteration).

*Business-partner security*. A supply-chain security program must ensure that any supply chain partner, as well as any further sub-contracted suppliers or logistics service providers, employ practices to ensure the security of all shipments. Any partner used in the manufacturing, packaging, or transportation of shipments must have documented processes for the selection of sub-contractors to ensure they can provide adequate supply-chain security. Suppliers should ensure that any parties handling shipments be knowledgeable of and able to demonstrate through written or electronic communication that they are meeting security guidelines. An example of contract language that could be used with freight forwarders and transport providers is contained in Appendix 5.2.

*Conveyance security.* Transportation, particularly drayage (inland truck support), may be the most vulnerable point of the supply chain. Procedures that suppliers and shippers should follow include inspection and sealing of containers (cf. ISO 17712:2010 on sealing containers), storage of containers, and shipment routing through freight forwarders or carriers who are certified in a recognized supply-chain security program or who otherwise demonstrate compliance with a firm's SCRM guidelines.

## *Responding to Events*

Even with the best laid plans, enterprises may still confront crises in their supply chains. We characterize crises as events that threaten the organization, with intense time pressures, high stress, and the need for rapid but careful decision making. A *crisis* is an unstable condition involving an impending abrupt or significant change that requires urgent attention and action to protect life, assets, property, operations or income, the environment and reputation. Crisis events include natural disasters, major infrastructure failures, major fires, political unrest, labor disputes, pandemics, information technology failures, or security threats (Figure 5.1).


Credit: Photo of suspected pirates surrendering to crew members of the Coast Guard Cutter Boutwell by Tyson Weinert,

## *Figure 5.1: Piracy in Regions of Unrest Can Pose Threats to Supply Chains*

*Crisis Management* comprises the overall strategic and tactical responses of an organization to recognize and respond effectively, efficiently and comprehensively to actualized threats. It involves **proactive** measures to detect, respond to, and recover from a crisis event. Crisis Management preparation and response activities are characterized by several phases:

- Preparation
- Response (consisting of Risk Assessment, Critical Incident Planning, Risk Mitigation, Emergency Response and Communications to Internal and External Stakeholders and Media Relations)
- Recovery and Business Resumption
- Testing, Training and Plan Maintenance

These processes are intended to enhance existing response capabilities by establishing a crisis-management structure that will provide integrated and coordinated planning and response activities at all levels within an organization. They will also establish a common and consistent set of notification and activation thresholds. The structure and processes are designed to complement, not supersede, emergency response plans and procedures at various functional organization units and facilities. When an incident occurs, these units and facilities will follow established local response plans and procedures.

Figure 5.2 presents a notional hierarchy for a crisis-management team in a large manufacturing firm. Should a local incident-response team not be able to manage a crisis, it would activate a broader manufacturing crisis management team (MCMT) that considers crises throughout the supply chain. If necessary, the MCMT would activate a theater crisis management team (TCMT), responsible for regional incidents affecting an enterprise and its employees. Above the TCMT and to be activated as needed are a corporate crisis-management team (CCMT) and an executive crisis-management team (ECMT).

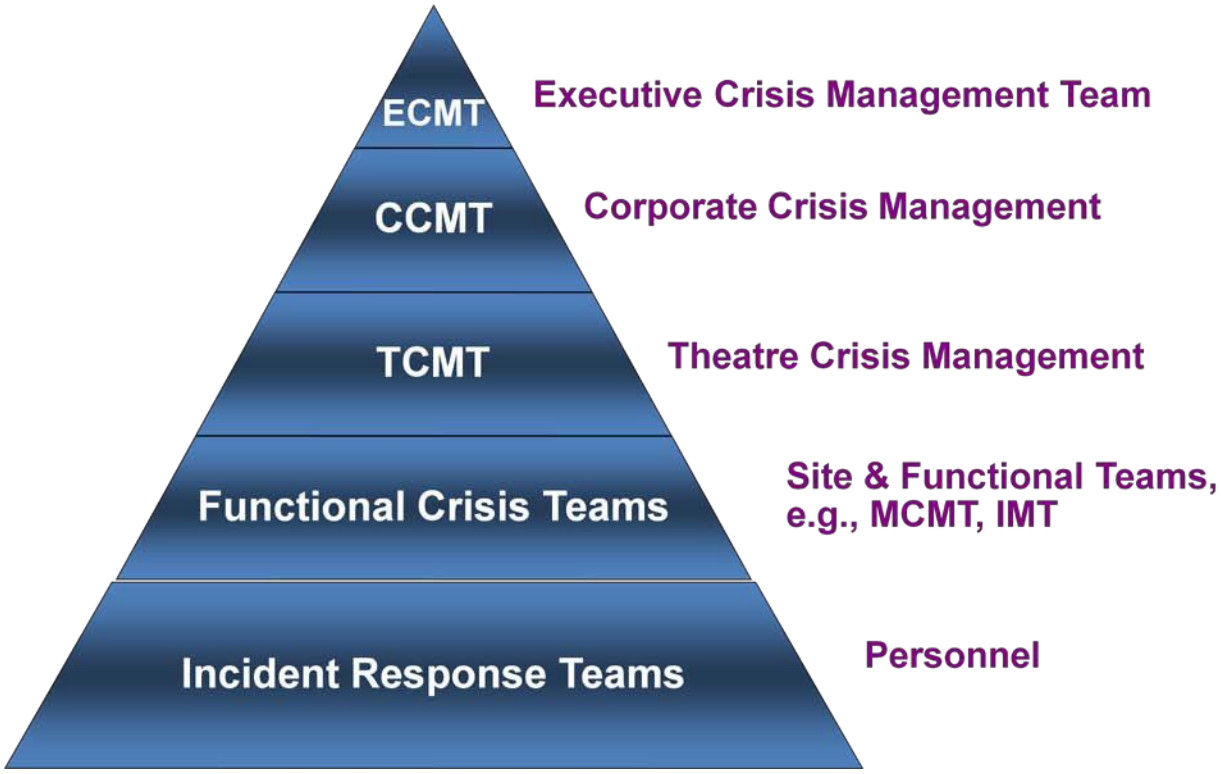



***Figure 5.2: Notional Crisis Management Structure and Engagement Model***

Incidents with high severity can quickly touch crisis teams throughout a global firm. For example, the H1N1 swine flu pandemic, which originated in Mexico, led to simultaneous activation of the MCMT and relevant TCMT for one leading firm. Within three days, the CCMT was activated and held regular briefings with the ECMT. Crisis management bridges activities that respond to an *emergency* (any incident that can threaten human life, health, property, or the environment if not controlled, contained, or eliminated immediately through local level response) and those supporting the organization's *recovery* (prioritized actions to return the organization's processes and support functions to operational stability) and *resumption* (restarting defined business processes and operations to a predetermined level) of operations.

Figure 5.3 presents a more generic process of how an MCMT might approach an incident. Members of the MCMT continually *monitor* the supply chain for potential risks. Should an event occur, members *assess* its consequence by making direct contact with suppliers in a region or through direct feedback from suppliers, partners, or customers.

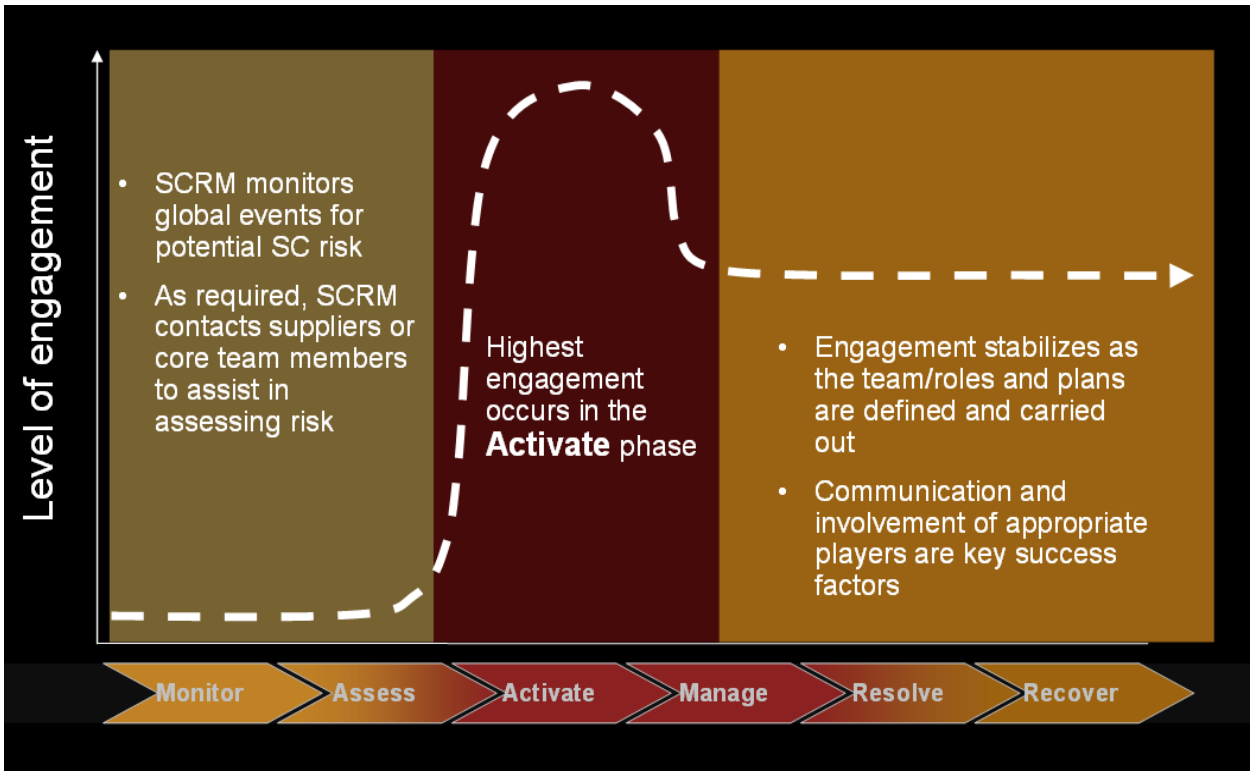



***Figure 5.3: MCMT Activation and Work Cycle***

An ideal crisis-response process should include the following steps, as depicted in Figure 5.4. (Appendix 5.3 provides a core-elements checklist for a crisis-management program.)

1. Crisis identification – recognition that the incident could significantly affect the organization and require additional resources to support local efforts.
2. Fact finding – gather sufficient factual information to prepare a risk assessment.
3. Risk Assessment - assess the potential seriousness and impact of the event.
4. Crisis Team activation and Critical Incident planning – assemble the appropriate internal and external team to provide strategic and tactical support to mitigate or resolve the event. At this point, the team may decide that the event can be adequately addressed with local resources and return event control to the local emergency response team.
5. Communication to stakeholders - if the event cannot be resolved locally, the Crisis Team will then establish a schedule to provide periodic communications to employees, customers, suppliers, financial organizations, stockholders and news media.
6. Event control and resolution – the Crisis Team, using local resources, will periodically assess remaining risk, provide necessary resources, and communicate with stakeholders until such time as the crisis is contained. This phase encompasses business recovery and resumption.
7. Post Incident review – once the crisis is contained, the Crisis Team will review and analyze the organization's response to the event. This may consist of two stages; a "hotwash" performed immediately after the event, followed by a formal debrief within 5 days. Crisis Team participants should be prepared to evaluate in detail the organization's response to determine what was done well and opportunities for improvement. It should then schedule and assign improvement actions.
8. Plan Maintenance, Training and Preparation – the organization should incorporate lessons learned into its crisis-management plan and distribute the updated plan to Crisis Team members and appropriate stakeholders. It should

also provide training on the plan and test it periodically to ensure that the organization is prepared for future events. (Appendix 5.4 provides a sample site-crisis plan.)

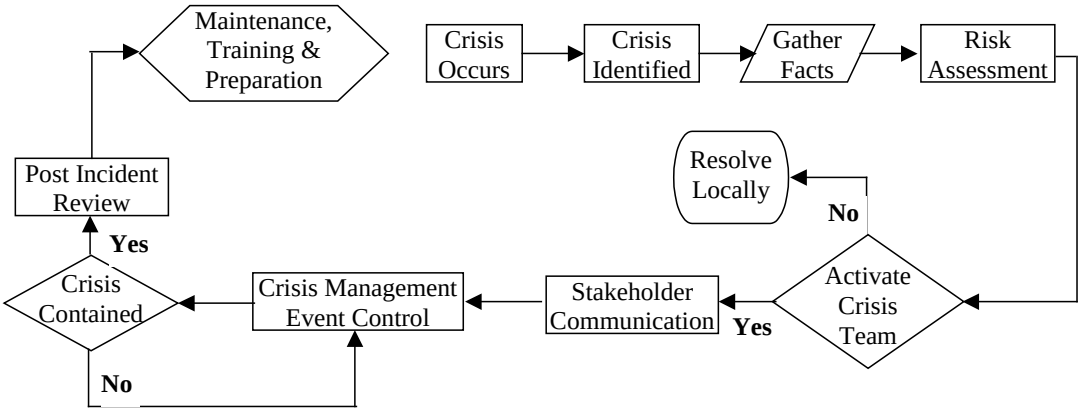



***Figure 5.4: Ideal Crisis Response Process***

If the incident is sufficiently severe, the MCMT will *activate*, assuming control of the situation, defining the risk, and developing the appropriate response. The team may *manage* the response through briefings and communications with senior staff, customer service personnel, and others as needed. The team has *resolved* the incident once it has a clear path to *recover* operations back to normal capacity. Recovery, as we discuss below, can take a few hours or many weeks.

## *Continuity of Operations and Recovery*

Business continuity planning comprises those activities, programs, and systems developed and implemented prior to an incident that are used to mitigate, respond to, and cover from supply-chain disruptions, disasters, or emergencies. It is an ongoing process, not a one-time project. A complete and tested plan gives an organization the framework to respond to respond effectively to an emergency, focus on protecting employees and property, communicating to key stakeholders, and recovering and restoring the most critical business activities within an acceptable time. These plans should be integrated and tested alongside those of the relevant critical suppliers, customers and other key stakeholders.

To be effective, business-continuity planning (also referred to as business-continuity management) should be an integrated management process supported from the top levels and managed at both organizational and operational levels. A business-continuity planning team should also establish company risk-tolerance levels and recovery priorities, validate business-recovery strategies, designate team members from each critical business function, ensure planning and documentation meets established timelines, and conduct periodic evaluation of the business-continuity planning program as based on performance objectives.

Specific business-continuity planning programs might include employee assistance, business-impact analysis, emergency-response planning, crisis-management planning, and business-recovery planning. We review each of these below.

Employee assistance programs help protect what are typically the top asset and therefore the top priority of a firm, its employees. Employee assistance programs, typically offered with a health-insurance plan, can help employees deal with personal problems that might adversely affect their work, health, and well-being. Such plans generally include assessment, short-term counseling, and referral services for employees and their household members. They may also offer housing assistance and salary advances.

Emergency response planning provides procedures to follow immediately after any emergency. Its objective is to protect employees, visitors, and property at business sites. Among other elements, it should include procedures for reporting emergencies, activating the plan, evacuating employees, activating an emergency operations center, updating lists of emergency contacts, assessing damage, repairing and restoring facilities, and testing emergency procedures.

One part of business-continuity planning, business-recovery planning, should include information on who needs to act, what needs to be done where, and when tasks need to be done to help resume operations. For example, for data center operations, the recovery plan should describe steps needed to recover and restore information technology infrastructure and services in case of site disaster. Disasters can destroy communications centers, necessitating their re-establishment (Figure 5.5). This should include data backup and hardware redundancy or replacement plans. The plan should identify and rank applications that support critical business activities. (Critical data, in turn, should be backed up daily and stored offsite weekly.)

Credit: SCRLC member company.

***Figure 5.5: Restoring Communications Can be Key to Resuming Operations***

# 6. Continual Monitoring of Risks and Their Treatment

Once an organization has established an SCRM program, including processes for identifying and treating risks, it should implement a monitoring program, evaluating plans, procedures, and capabilities through periodic review, testing, post-incident reports, and other exercises. It should check conformity and effectiveness of the program, establish, implement, and maintain procedures for monitoring and taking corrective action as necessary. This includes reviewing other organizational changes that may affect SCRM.

Above all, organizations should test their plans periodically. Workers learn best by doing, hence regular testing of business-continuity plans is necessary to ensure they will work when needed. Organizations may test plans in four ways, including

- an orientation or "walk-through" to acquaint teams with the plan and their roles and responsibilities in it.
- a "tabletop" exercise to reinforce the logic and content of the plan and to integrate its decision-making processes and provide "hands-on" experience. This may entail presenting a team with a scenario and related events posing problems to solve. The exercise is designed to provoke constructive discussion and familiarize participants with the plan, their roles and responsibilities, and possible gaps in the plan.
- a functional test that creates simulations involving group interaction in actual disruptions in order to validate the key planning components and strategies. Such tests may include evacuation procedures.
- a full-scale test to evaluate the plan and response through interaction of suppliers and supply-chain partners.

Plans should be tested at least annually and preferably more often. Some organizations may concentrate on testing evacuation procedures which, while critical, can exclude other elements.

Plans, like risks necessitating them and risk treatments, should be monitored over time. In the next section, we review the process of monitoring risks and risk treatment, and discuss as well how firms may wish to monitor one particular form of risk, that posed by changing government regulations.

## *Testing and Adjusting the Plan*

The goals and expectations of testing and exercises should include

- Determining whether a crisis-response process works and how it can be improved
- Testing capacity (e.g., abilities of an emergency phone system)
- Reducing time to accomplish a process (e.g., repeating drills so as to shorten response time)
- Increasing awareness and knowledge among employees about the risk-management plan
- Incorporating lessons learned from previous tests and actual incidents.

Testing should occur at regularly scheduled intervals. It should evolve over time, starting as a relatively simple program but becoming increasingly complex as testing needs develop further. It should involve suppliers, customers and other

stakeholders as appropriate. The process should be embedded within the procurement contract terms and integrated into the supplier management processes.

Figure 6.1 provides a framework for exercises and testing. Testing, like the SCRM process, begins with establishing the context, but, also like the SCRM process, is a cyclical process. Both involve planning, following through on the plans, checking their performance, acting to improve their performance, and reconsideration of how the results, as well as considering changes in the organizational context and how they might reshape the context, scope, and boundaries of SCRM for an organization.

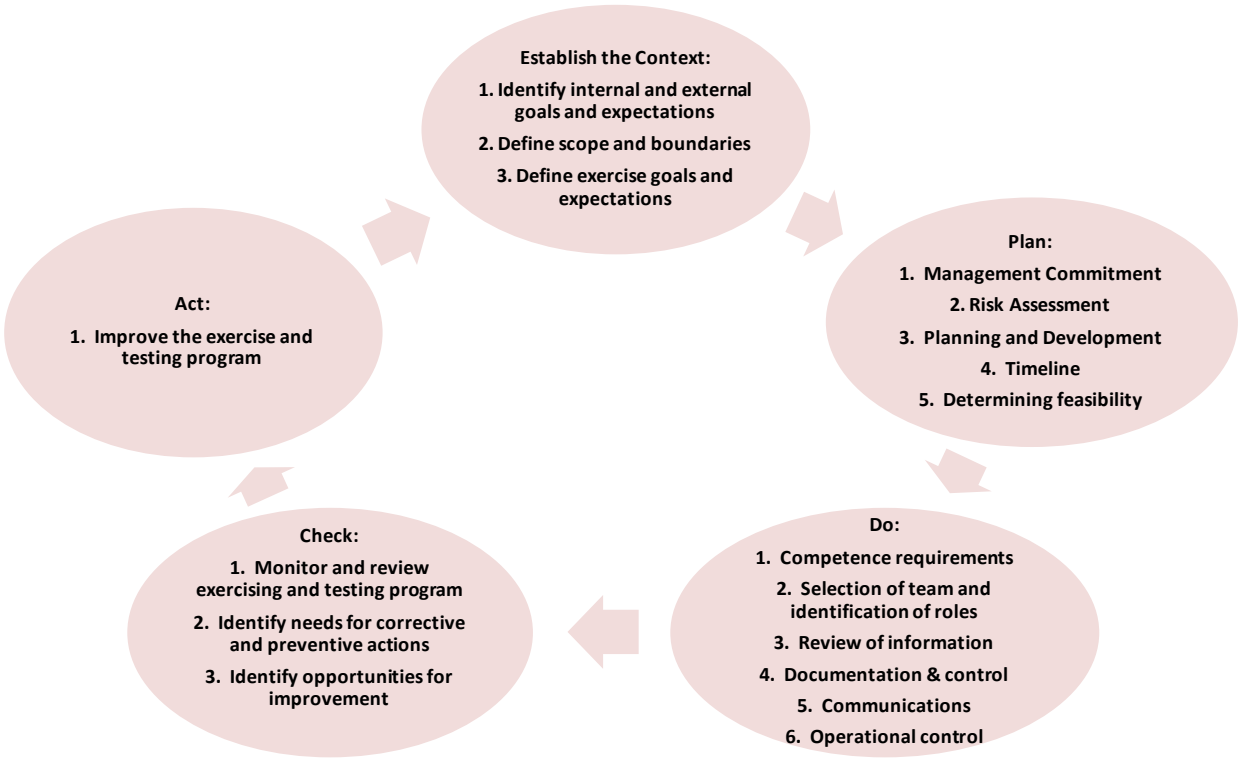



***Figure 6.1: Framework for Exercises and Testing***

Testing, evaluating, and adjusting their SCRM programs can help organizations ultimately strike a balance between being able to respond to events while appropriately focusing resources to address the most likely and damaging risks (Hepenstal and Campbell, 2007). In the first phase of developing a program, an organization may respond to corporate directives to increase some elements of security, with corporate leadership itself often responding to an external event (Figure 6.2). In the second phase, crisis management teams may form and develop and test more extensive plans for responding to risks and events resulting from them. In the third phase, teams may become more proactive in assessing vulnerabilities and prioritizing them for mitigation efforts. In the fourth phase, organizations will have in place plans for critical materials and key vulnerabilities, and employees will realize business continuity preparations are an essential part of their work. In the fifth phase, organizations will continually assess risks, prioritize them, and make appropriate risk-mitigation efforts, striking a balance between risks and resources available to address them.


**Source: Hepenstal and Campbell, 2007**

***Figure 6.2: Evolution of Business Continuity Planning at One Organization***

The experiences of one global corporation in responding to Hurricane Katrina in the United States in August 2005 and to Typhoon Milengo in September 2006 help illustrate how organizations can adapt and improve their responses to a common type of risk over time (Hepenstal and Campbell, 2007). While the organization had advance notice for both storms, for Katrina it only triggered its crisis response team once noticing a manufacturing facility for a key supplier was underwater. Between Katrina and Milengo, the organization developed an ability to identify critical suppliers with manufacturing facilities in the path of storms, including abilities to evaluate potential consequence and determine appropriate mitigation strategies as well as to determine appropriate mitigation strategies. As a result, before Milengo hit the Philippines, the organization had already begun mitigation efforts.

## *Areas of Continual Adjustment*

Some risks, such as those posed by hurricanes and typhoons, may not change much over time. Other risks that organizations face, such as those inherent in their processes, suppliers, or their regulatory environment, can change. As a result, firms need to monitor risks and how to address them over time. As just one example of this, below we review the nature of regulatory risks and how organizations can respond to and monitor it.

While perhaps not obvious at first, regulations can create significant supply-chain risks. They can affect import and export documentation and compliance requirements, as well as shipment safety and security issues, and thereby affect shipment costs and create risk for delays and financial penalties. Regulations can affect the countries or states in which an organization may work, as well as those in which its suppliers may work.

Some recent examples of U.S. regulations affecting supply-chain processes include the requirement of the Transportation Security Administration for screening of all cargo on passenger jets, U.S. Customs and Border Protection's requirement for new data elements on the Importer Security Filing (ISF) regulation for all ocean shipments, and Customs regulations requiring use of a high-security bolt seal on all ocean shipments. The air-cargo screening requirement adds costs for new screening facilities as well as new risks of delay at points where adequate screening capacity might not exist. The ISF reporting requirement adds costs for compliance and shipment-delay risks if reporting is not done properly. The high-security bolt requirement can also add risk of delays or even rejection of a shipment should shippers fail to comply. Compliance failure in any of these or other regulations could also result in financial penalties, embarrassing news coverage, or even loss of license to do business.

In sum, failure to monitor, shape, and respond to new regulations can pose significant risks for the supply chain. Below we present some guidelines and best practices for an organization seeking to minimize such risks. Like all recommendations in this document, these are meant primarily as guidelines to provoke thought, and from which organizations may wish to select for adaptation to their own circumstances. An effective risk-mitigation program for legislative and regulatory requirements should help an organization monitor proposed or pending regulations, participate in the process shaping final regulations, plan and respond to changes in regulation, avoid compliance penalties, and ensure the smooth flow of incoming and outgoing shipments.

In monitoring risks, organizations should seek to become aware early of proposed legislative and regulatory initiatives, understand how they might affect their business, and share with internal decision makers to determine a response. Some means to do this include establishing a “government affairs” function or assigning individual responsibility to monitor proposed legislation and regulations, creating an internal network of individuals who monitor regulatory issues, joining trade associations that monitor these and subscribe to their newsletters and bulletins, and developing other external contacts to monitor legislative and regulation changes. Monitoring should include assessing the risk of newly emerging regulation, tracking compliance with existing regulations, and identifying the points of the supply chain that will be affected by regulations. Appendix 6.1 provides some sample regulatory and compliance requirements, points along the supply chain they may affect, and what control, if any, an organization may have over them.

To shape regulations, organizations should seek to participate in the legislative and rulemaking process. They may develop an internal process for tracking and responding to regulatory notices, using this process to identify the consequences of new regulation and to offer preferred alternatives. They might establish an internal capacity, or hire an external consultant or lobbyist, to represent the organization in the development of legislative or regulations. Joining and participating in industry associations provides another means for interacting with political or government-agency leaders who shape legislation and regulations. Organizations may seek opportunities for volunteering to participate on industry advisory committees” or other outreach events that government agencies use in developing and seeking feedback on regulatory changes.

In responding to regulations, organizations should prepare in advance to avoid or mitigate the risks, including costs, delays, and penalties inherent in new regulations. While monitoring and seeking to shape pending regulatory requirements, organizations should develop, with early executive support and funding, an internal process or team of cross-functional representatives to analyze pending regulations and plan how to address each. For new regulations, organizations must communicate details to partners and help them otherwise prepare to support the new requirements. New requirements may also require organizations to update their contractual terms and conditions with their supply-chain partners. Developing and implementing plans to monitor the supply chain as new regulations go into effect can ensure that compliant processes are in place and working.

New regulations, like other evolving areas with which an organization must contend, can create significant risks for supply chains. These risks may range from costs to delays to compliance penalties to still other areas. To be resilient, a supply chain must have the capacity to monitor, shape, and respond to evolving areas such as new regulations.

## *Summary*

Effective supply-chain risk management (SCRM) is essential to a successful business. As globalization increases, so too do the critical interdependencies and complexities between suppliers, logistics providers, and a successful enterprise. A breakdown in any part of the supply chain connecting these entities can potentially lead to catastrophic consequences.

We hope that the guidelines in this paper assist you in the crucial task of establishing an effective supply chain risk management program tailored to the unique characteristics of your business. These principles should be integrated into the other key corporate procedures and policies you follow for procurement and general risk management including supplier-management routines.

While no risk management program can fully predict, mitigate, or prevent all risks or consequences, companies that proactively implement a supply-chain risk-management program will be more resilient and prepared for the day when a "risk" becomes "real."

The Supply Chain Risk Leadership Council welcomes your feedback on and suggestions for this SCRM Best Practices Guide. Please forward your comments to: info@scrlc.com.

# Appendixes

## *Appendix 2.1: Sample Risks by Category*

- External, End to End Supply Chain Risks
  - Natural Disasters
    - Epidemics
    - Earthquakes
    - Tsunamis
    - Volcanoes
    - Weather disasters (hurricanes, tornados, storms, blizzards, floods, droughts)
  - Accidents
    - Fires
    - Explosions
    - Structural failures
    - Hazardous spills
  - Sabotage, Terrorism, Crime, and War
    - Computer attacks
    - Product tampering
    - Intellectual theft
    - Physical theft
    - Bombings
    - Biological and chemical weapons
    - Blockades
  - Government Compliance and Political Uncertainty
    - Taxes, customs, and other regulations
    - Compliance issues
      - Regulatory financial reporting (e.g., Sarbanes-Oxley)
      - Operations
      - Logistics / Trade
      - Regulatory Approvals - Marketing Approvals
      - Public Health
      - Environmental
      - Trade restrictions (e.g., Buy American Act)
      - Regulatory Audit history
    - Currency fluctuations
    - Political unrest
    - Boycotts

- Labor Unavailability and Shortage of Skills
  - Availability
  - Quality
  - Cost
  - Unrest
  - Strikes and slowdowns
- Industry-wide (i.e., Market) Challenges
  - Capacity constraints
  - Unstable prices
  - Lack of competition
  - Entry barriers
  - Capital requirements
  - Specific assets
  - Design patents
  - Process patents
  - Shrinking industry
  - Low supplier profitability
  - Certification
  - Cost trends
  - Recessions/Inflation
- Lawsuits
  - Environmental
  - Health and safety
  - Intellectual property
- Technological Trends
  - Emerging technologies (pace/direction)
  - Obsolescence
  - Other technological uncertainty

Supplier Risks: External, contract manufacturers, or internal business unit

- Physical and Regulatory Risks
  - Key Suppliers Located in High Risk Areas
  - Material Unavailability/Poor Planning
    - Raw materials
    - Other materials
  - Legal Noncompliance / Ethical practices
    - Labor practices
    - Safety practices & performance
    - Environmental practices
    - History & outcomes of lawsuits
    - Tax practices
  - Regulatory Noncompliance
    - Customs/trade

- Security clearance requirements
- History & outcomes of regulatory audits
- Regulatory certification requirements (e.g., Food & Drug Administration, Federal Aviation Administration)
- Critical disclosure – International Traffic & Arms Regulations

Production Problems

- Capacity
  - Too little, too much, or diminishing
  - Order and shipping times
  - Out of stock (i.e., no/low inventory)
  - Performance history, equipment age & downtime (manufacturing & testing equipment)
  - Repair cycle time
- Inflexible Production Capabilities (Long setup times)
- Technological Inadequacies or Failures
  - Incompatible information systems
  - Slow adoption of new technology
- Poor Quality
  - Defects / contamination in manufactured product
  - Mislabeling of items
  - Lack of training or knowledge
- Lead Times
  - Backlogs
  - Unresponsive
  - Unreliable
  - Variable

Financial losses and premiums

- Degree of Competition/Profitability
  - Downstream integration or too much competition
  - Little/no competition - sole source
  - Mergers & Acquisitions
- Financial Viability
  - Inability to sustain in a downturn
  - Bankruptcy
  - Withdrawal from the market

Management Risks

- Inadequate Risk Management Planning
  - Lack of business continuity plans
  - Lack of requirements for supplier's supplier business continuity plans
- Management Quality
  - High turnover
  - Dishonesty
  - Poor labor relations

- Poor metric scorecards
- Substituting inferior or illegal materials/parts
  - Failing to perform required treatments/tests
  - Submitting inaccurate/false invoices
- Lack of Continuous Improvement
  - Unwillingness
  - Cost escalation
  - Opaque processes
  - Opportunistic behavior
  - Inflation of purchase costs
- Dependence on One or a Few Customer(s)
- Poor Communication
  - Internal
  - External
  - Transparency of data & operations

Upstream (i.e., subcontractors and their subcontractors) Supply Risks

- Any of the above external/supplier risks
- Lack of visibility into subcontractors
- No or poor relationships with subcontractors
- Diminishing sources of supply
- Transition “costs” for new suppliers

Distribution Risks/Disruptions: Inbound or Outbound

Infrastructure Unavailability

- Roads
- Rails
- Ports
- Air capacity/availability

Assets - Lack of Capacity or Accidents

- Containers
- Trucks
- Rail cars
- Ships
- Airplanes

Labor Unrest/Unavailability

- Truck drivers
- Rail operators
- Longshoremen
- Pilots

Cargo Damage/Theft/Tampering

- Physical damage
- Theft and other security problems
- Tracking the damage

- Environmental controls (e.g., temperature, humidity)
- Warehouse Inadequacies
  - Lack of capacity
  - Inaccessibility
  - Damage
  - Environmental controls (e.g., temperature, humidity)
  - Lack of security
- IT System Inadequacies/Failures
- Long, Multi-Party Supply Pipelines
  - Increased chance of all problems above
  - Longer lead time

Internal, Enterprise Risks

- Operational risk
  - Loss of Inventory (damage, obsolescence)
  - Equipment loss, mechanical failures
  - Process Issues
    - Process reliability
    - Process robustness
    - Lead time variability
    - Inflexible Production Capabilities (long set up times, etc)
  - Capacity
    - Too little, too much, or diminishing
    - Order and shipping times
    - Out of stock (i.e., no/low inventory)
    - Performance history, equipment age & downtime (manufacturing & testing equipment)
    - Repair cycle time
  - Poor Quality
    - Defects in manufactured product
    - Failure to maintain equipment
    - Lack of training or knowledge
  - Environmental performance to permits / other
- Government Compliance and Political Uncertainty
  - Taxes, customs, and other regulations
  - Currency fluctuations
  - Political unrest
  - Boycotts
- Demand Variability/Volatility
  - Drawdown of the stockpile
  - Exceeding maintenance replacement rate
  - Shelf life expiration
  - Surges exceed production, repair, or distribution
  - Shortfalls

Personnel Availability/Skills Shortfalls
- Sufficient number
- Sufficient knowledge, skills, experience
- Union contract expiry
- High turnover rate

Design Uncertainty
- Changes to requirements
- Lack of technical detail
- Lack of verification of product
- Changes to product configuration
- Poor specifications
- Reliability estimates of components
- Access to technical data
- Failure to meet design milestones
- Design for supply chain (e.g., obsolescence, standardization, and commonality)

Planning Failures
- Forecast reliability/schedule availability
- Planning data accuracy
- Global visibility of plans & inventory positions
- Competition/bid process
- Acquisition strategy
- Manufacturability of a design
- Program maturity
- Subcontracting agreements

Financial Uncertainty/Losses
- Funding availability
- Workscope/plan creep
- Knowledge of supplier costs
- Strategic risk

Facility Unavailability/Unreliability/ Capacity
- Facility breakdown
- Mechanical failures
- Sites located in high risk areas
- Adequate capacity

Testing Unavailability / Inferiority / Capacity
- Unreliable test equipment
- Operational test qualifications
- Operational test schedule
- Integration testing
- Transition from first test to mass production

Enterprise Underperformance/Lack of Value
- Customer satisfaction/loyalty

- Liability
- Cost/profit
- Customer demand
- Uniqueness
- Substitutability
- Systems integration
- Other application/product value

Supplier Relationship Management (SRM) Use

- Contract/supplier management availability and expertise
- In-house SRM expertise
- Lack of internal and external communication/coordination
- Supplier development and continuous improvement
- Supplier communications - (EDI web, real time demand, plans, forecasts, technology roadmaps)

# *Appendix 4.1: Sample Contractual Terms and Conditions for Supply-Chain Security*

Your company should ensure that proper contractual terms and conditions are in place requiring your suppliers and logistics partners to comply with proper supply chain security procedures as follows:

**SAMPLE SUPPLIER Terms and Conditions:**

For those Goods ordered by Buyer from Seller that are shipped directly to Buyer, Seller agrees to comply with the following supply chain security requirements from the Point of Origin as provided below. The Point of Origin is the site where such Goods are assembled, manufactured, packaged and shipped.

Seller shall include this provision with applicable Subcontractors. For purposes of this provision, Subcontractors shall be defined as those sub-tier manufacturers or suppliers from which the shipment of Goods is shipped directly from said manufacturers or supplier's facilities to Buyer and those suppliers engaged in packaging or transport of Buyer shipments (including but not limited to freight forwarders, 3rd party logistic companies, packagers). Seller shall be responsible to Buyer for any breach of such requirement by its subcontractor.

**A.** Supplier will maintain adequate security controls and procedures as further described in this Section 6.I.A.

- **a. Seller Subcontractor Selection Process:** Seller shall have documented processes for the selection of its Subcontractors. The process shall ensure that such Subcontractors maintain adequate security controls and procedures.
- **b. Physical Security:** Facilities must be protected against unauthorized access including but not limited to cargo handling and storage facilities which shall have physical security deterrents.
  - i. All entry and exit points for vehicles and personnel shall be controlled.
  - ii. Secure all external and internal windows, gates, and doors through which unauthorized personnel could access the facility or cargo storage areas with locking devices.
  - iii. Provide adequate lighting inside and outside facilities to prevent unauthorized access.
- **c. Access controls**: Prevent unauthorized entry into facilities using access controls which may include but are not limited to badge readers, locks, key cards, or guards.
  - i. Positively identify all persons at all points of entry to facilities.
  - ii. Maintain adequate controls for the issuance and removal of employee, visitor and vendor identification badges, if utilized.
  - iii. Upon arrival, photo identification shall be required for all non-employee visitors.
- **d. Personnel Security and Verification:** Screen prospective employees consistent with local regulations. Verify employment application information prior to employment.
- **e. Ocean Container and Truck Trailer Security:** Maintain container and trailer security to protect against the introduction of unauthorized material and/or persons into shipments. In the event containers are stuffed, inspections shall be made of all ocean containers or truck trailers prior to stuffing, including but not limited to the inspection of the reliability of the locking mechanisms of all doors.
  - i. **Ocean Container and Truck Trailer Seals:** Properly seal and secure shipping containers and trailers at the point of stuffing. Affix a high security seal to all access doors on truck trailers and ocean containers bound for the U.S. Such seals must meet or exceed the current PAS ISO 17712 standard for high security seals.
  - ii. **Ocean Container and Truck Trailer Storage:** Empty or stuffed ocean containers and truck trailers must be stored in a secure area to prevent unauthorized access and/or manipulation.
- **f. Information Technology (IT) Security**: maintain IT security measures to ensure all automated systems are protected from unauthorized access.
  - i. Use individually assigned accounts that require a periodic change of password for all automated systems.

ii. Maintain a system to identify the abuse of IT resources including but not limited to improper access, tampering or altering of business data and will discipline violators.

**g. Procedural Security**: maintain, document, implement and communicate the following security procedures to ensure the security measures in this clause are followed and must include:

i. Procedures for the issuance, removal and changing of access devices.
ii. Procedures to identify and challenge unauthorized or unidentified persons
iii. Procedures to remove identification, facility, and system access for terminated employees.
iv. Procedures for IT security and standards.
v. Procedures to verify application information for potential employees.
vi. Procedures for employees to report security incidents and/or suspicious behavior.
vii. Procedures for the inspection of ocean containers or truck trailers prior to stuffing.
viii. Procedures to control, manage, and record the issuance and use of high security bolt seals for ocean containers and truck trailers. Such procedures must stipulate how seals are to be controlled and affixed to loaded containers and shall include procedures for recognizing and reporting compromised seals or containers to Customs or the appropriate authority and Buyer.

**B.** Upon request, complete a Supply Chain Security Self Assessment Questionnaire.

**C.** Seller and its subcontractors shall be subject to periodic site visits by Buyer during normal operation hours, to confirm compliance with the terms contained within this clause.

**D.** Maintain procedures for employees to report security incidents and/or suspicious behavior. Immediately notify Buyer of any actual or suspected breach of security involving Buyer's cargo.

## *Appendix 5.1: Sample Supply-Chain Security Self-Assessment Questionnaire for Suppliers or Other Supply-Chain Partners*

Instructions:

On questions which require a yes or no answer, please circle yes or no, and then describe your answer in the space provided. If desired you may attach copies of documents that support your descriptions.

## General Information:

Contact Name:

Company Name:

Primary Location/Address:

Street:

City, State/Province, Postal Code:

Country:

Phone:

If you have multiple locations from which you ship to (your company), please list additional sites:

Please list your company contacts for Security and Transportation below.

Contact for Security:

Name:

Title:

Phone Number:

Email address:

Contact for Transportation:

Name:

Title:

Phone Number:

Email address:

Type of products produced for (your company) at your facility:

## Physical Security:

| | | | |
|---|---|---|---|
| 1 | Does your facility utilize security guards? | Yes | No |
| 1a | If yes, describe how they are positioned and the hours of coverage and areas of coverage within your facility that they provide. | | |
| | Additional Comments: | | |
| | | | |
| 2 | Is your facility fully enclosed by perimeter fencing or walls? | Yes | No |
| 2a | If yes, please describe the type of materials used and the height. | | |
| | Additional Comments: | | |
| | | | |
| 3 | Does your facility utilize security cameras for monitoring perimeters, entries and exits, loading bays, or other areas? | Yes | No |
| 3a | If yes, describe coverage provided and who monitors them | | |
| | Additional Comments: | | |
| | | | |
| 4 | Does your facility have locks on doors, windows and gates? | Yes | No |
| | Additional Comments: | | |
| | | | |
| 5 | Are the locks kept locked at all times to prevent unauthorized personnel from entering? | Yes | No |
| 5a | If no, please explain why. | | |
| | Additional Comments: | | |
| | | | |

| | | | |
|---|---|---|---|
| 6 | Do you have bars, screens, or other materials over the windows? | Yes | No |
| 6a | If yes, please describe what materials are used. | | |
| | Additional Comments: | | |
| | | | |
| 7 | Do you have an alarm intrusion system? | Yes | No |
| 7a | If yes, please describe who is monitoring the alarm and where the alarm sensors are located at. | | |
| | Additional Comments: | | |
| | | | |
| 8 | Is your facility exterior lighted/illuminated at night? | Yes | No |
| 8a | If yes, please describe what areas are illuminated. | | |
| | Additional Comments: | | |
| | | | |
| 9 | Is the shipping/receiving area secure at all times to prevent access by unauthorized personnel? | Yes | No |
| 9a | If yes, please describe what physical barriers are used and what personnel is allowed access. | | |
| | Additional Comments: | | |
| | | | |
| 10 | Are outgoing shipments stored in a separate area that is secure and prevents unauthorized access? | Yes | No |
| 10a | If yes, describe where the shipments are stored and who has access to them. | | |
| | Additional Comments: | | |

| | | |
|---|---|---|
| | | |
| | Please describe any aspects of physical security at your facility that you feel were not addressed above. | |

## Access Control:

| | | | |
|---|---|---|---|
| 1 | Do you use an employee badge system for entry and monitoring onsite activities? | Yes | No |
| 1a | If yes, describe the badge system (electronic, color coded, how many badges are needed to gain access, etc.) | | |
| 1b | If no, but you use another method to identify and track employees, please describe | | |
| | Additional Comments: | | |
| | | | |
| 2 | Do you have access controls in place at entry points to your facility? | Yes | No |
| 2a | If yes, describe what access controls are used at each point of access into your facility. | | |
| | Additional Comments: | | |
| | | | |
| 3 | Is vehicle access into your facility controlled? | Yes | No |
| 3a | If yes, describe how vehicle access is controlled and what vehicles are allowed access. | | |
| | Additional Comments: | | |
| | | | |
| 4 | Are vehicles and drivers screened or inspected prior to entry to your facility | Yes | No |
| 4a | If yes, describe the method of screening (driver ID checks, vehicle inspections, etc.) | | |

| | | | |
|---|---|---|---|
| | Additional Comments: | | |
| | | | |
| 5 | Do you identify, record, and track all visitors? | Yes | No |
| 5a | If yes, what method is used and how are the records kept? | | |
| | Additional Comments: | | |
| | | | |
| | Please explain any access controls at your facilities that you feel were not addressed above. | | |
| | | | |

## Personnel Security:

| | | | |
|---|---|---|---|
| 1 | Are employee work history background checks completed prior to hiring? | Yes | No |
| 1a | If yes, describe to what extent the background check is completed. | | |
| 1b | If no, describe if there is a local law that prohibits this action. | | |
| | Additional Comments: | | |
| | | | |
| 2 | Are employee criminal background checks completed prior to hiring? | Yes | No |
| 2a | If yes, describe to what extent the background check is completed. | | |
| 2b | If no, describe if there is a local law that prohibits this action. | | |
| | Additional Comments: | | |
| | | | |

| | | | |
|---|---|---|---|
| 3 | Are non-employee contractors allowed routine access into your facility (janitorial service, delivery drivers, food vendors, etc) | Yes | No |
| 3a | If yes, are employment and criminal background checks completed prior to access being allowed? | | |
| 3b | Is access restricted to these workers so that they may only access facilities that they need to be in? | Yes | No |
| 3c | Are these workers restricted from accessing the shipping and receiving areas? | Yes | No |
| 3d | Are these workers required to wear identification badges | Yes | No |
| | Additional Comments: | | |
| | | | |
| | Please explain any personnel controls at your facilities that you feel were not addressed above | | |
| | | | |

## Procedural Security:

| | | | |
|---|---|---|---|
| 1 | Is there a Security Manager and staff? | Yes | No |
| 1a | If yes, what is the person's name and how many staff are working security? | | |
| | Additional Comments: | | |
| | | | |
| 2 | Are physical security procedures documented? | Yes | No |
| | Are access control security procedures documented? | Yes | No |
| | Are I.T. security procedures documented? | Yes | No |
| | Are personnel security procedures | Yes | No |

| | | | |
|---|---|---|---|
| | documented? | | |
| | Are education/training of security procedures documented | Yes | No |
| | Additional Comments: | | |
| | | | |
| 3 | Are there procedures for employees reporting security problems and addressing the situation? | Yes | No |
| | Additional Comments: | | |
| | | | |
| 4 | Are there procedures for marking, counting and weighing outgoing shipments? | Yes | No |
| | Additional Comments: | | |
| | | | |
| 5 | Are there procedures for documenting outgoing shipments? | Yes | No |
| | Additional Comments: | | |
| | | | |
| 6 | Are there procedures for storing and identifying incoming and outgoing shipments? | Yes | No |
| | Additional Comments: | | |
| | | | |
| 7 | Are there procedures in place for storing shipment documentation (packing list, commercial invoice, etc.) | Yes | No |
| | Additional Comments: | | |
| | | | |
| 8 | Are procedures in place for securing outgoing shipments against intrusion? | Yes | No |
| | Additional Comments: | | |

| | | | |
|---|---|---|---|
| | | | |
| 9 | Does a 3rd party physically pack these shipments? | Yes | No |
| 9a | If yes, are security procedures flowed down to the packers? | | |
| | Additional Comments: | | |
| | | | |
| **If ocean and/or truck trailer containers are used, please answer questions 10 - 12.**<br><br>**If not, skip to question 13.** | | | |
| | | | |
| 10 | Are containers examined prior to loading to ensure no explosives or other contraband is present? | Yes | No |
| 10a | If yes, describe the process. | | |
| | Additional Comments: | | |
| | | | |
| 11 | Describe how ocean containers (full and/or empty) are stored. | | |
| | Additional Comments: | | |
| | | | |
| 12 | Are high security bolt seals used on ALL ocean/truck trailer container entry doors? | Yes | No |
| 12a | If yes, How are bolt seals controlled? (e.g., storage and procedures to assure no fraudulent use). | | |
| | Additional Comments: | | |
| | | | |
| 13 | What security considerations have been established for selecting and screening carriers that are providing transportation services for outgoing shipments? | | |

| | | | |
|---|---|---|---|
| | Additional Comments: | | |
| | | | |
| 14 | Are there procedures for reporting problems/delays in the movement of cargo? | Yes | No |
| 14a | If yes, describe the process. | | |
| | Additional Comments: | | |
| | | | |
| 15 | Describe the materials used for packing products that are being sent to Boeing (e.g., cardboard box, container, etc). | | |
| 15a | Are tamper evident materials used? | | |
| | Additional Comments: | | |
| | | | |
| | Please explain any procedural controls at your facilities that you feel were not addressed above | | |
| | | | |

## Education and Training:

| | | | |
|---|---|---|---|
| 1 | Does your company provide a security awareness program related to protecting product integrity and facility security | Yes | No |
| 1a | If yes, please describe what is covered in this training and awareness program. | | |
| 1b | If yes, how often are employees required to take this training and awareness program? | | |
| | Additional Comments: | | |
| | | | |

| | | | |
|---|---|---|---|
| 2 | Is your company certified in a supply chain security or known shipper/consignor program? (e.g. AEO, PIP, etc.) | Yes | No |
| 2a | If yes, indicate which program you have certification in, when it was obtained, and who provided the certification. | | |
| | Additional Comments: | | |
| | | | |
| 3 | Do you require cargo integrity training for employees in the shipping and receiving areas and opening mail? | Yes | No |
| 3a | If yes, how often is this training required? | | |
| | Additional Comments: | | |
| | | | |
| 4 | Do you require education on recognizing internal conspiracies and protecting access controls for all employees? | Yes | No |
| 4a | If yes, how often is this training required? | | |
| | Additional Comments: | | |
| | | | |

## *Appendix 5.2: Sample Supply-Chain Security Contract Language for International and Third-party Logistics Service Providers*

For those Goods which are distributed, handled, warehoused, transported or shipped by Service Provider to (your company), Service Provider agrees to comply with the provisions of this section. For purposes of this section, 3PL includes Service Providers and means any outsourced Service Provider that provides services (e.g. distribution, handling, warehousing, transportation or shipping) for (your company) shipments.

Service Provider shall ensure that Subcontractors comply with the terms of this section and shall include these terms and conditions in any Subcontractor contracts. For purposes of this section, Subcontractors shall be defined as those sub-tier service providers of Service Provider which are involved in the distribution, handling, warehousing, transportation and shipping of (your company) shipments (including but not limited to freight forwarders, 3rd party logistic companies, packagers, local trucking/transport companies). Service Provider shall be responsible for any breach of this section by its Subcontractors.

**A. Supply Chain Security Compliance:** Service Provider must ensure that all Service Provider and applicable Subcontractor facilities involved in the distribution, handling, warehousing, transporting or shipping of (your company) goods meet all security standards documented below and all applicable local regulations. Service Provider should maintain certification in an official supply chain security program (C-TPAT, AEO, etc) and comply with those respective security standards throughout the period of this Agreement. Service Provider's loss of certification or failure to sustain appropriate security standards or breach of this section will be grounds for termination of this Agreement.

**B. Supply Chain Security Program Status:** Prior to execution of this Agreement, Service Provider will send a letter verifying its supply chain security certification in any official program it participates in. Service Provider will immediately notify (your company) of any change to its certification status.
If not certified, Service Provider must complete a Security Questionnaire to confirm that its procedures and security measures comply with minimum supply chain security criteria. Service Provider will send copies of the aforementioned Security Questionnaire to (your company).

**C. C-TPAT Certification:** Service Provider agrees to use certified Subcontractors to the extent available. In the absence of certified Subcontractor, Service Provider may use companies (including local cartage companies) that have agreed in writing to follow these supply chain security guidelines and will promptly notify (your company) of such usage. If no certified transport and handling providers or companies that have agreed to follow these security guidelines are available to move (your company) shipments, Service Provider will contact (your company) immediately for direction.

**D.** Service Provider will maintain adequate security controls and procedures as further described in this section.

1. **Supply Chain Security Program:** Service Providers are encouraged to participate in and will advise (your company) of its participation in national supply chain security programs including, but not limited to. Partners in Protection (“PIP”) and Authorized Economic

Operator ("AEO") and shall list the countries and extent of participation. Service Provider shall provide prompt notice of any changes to its supply chain security program status.

2. **Service Provider Subcontractor Selection Process:** Service Provider shall have documented processes for the selection of its Subcontractors. The process shall ensure that such Subcontractors maintain adequate security controls and procedures.

3. **Physical Security:** Facilities must be protected against unauthorized access including but not limited to cargo handling and storage facilities which shall have physical security deterrents.
   - **a.** All entry and exit points for vehicles and personnel shall be controlled.
   - **b.** Secure all external and internal windows, gates, and doors through which unauthorized personnel could access the facility or cargo storage areas with locking devices.
   - **c.** Provide adequate lighting inside and outside facilities to prevent unauthorized access.

4. **Access controls**: Prevent unauthorized entry into facilities using access controls which may include but are not limited to badge readers, locks, key cards, or guards.
   - **a.** Positively identify all persons at all points of entry to facilities.
   - **b.** Maintain adequate controls for the issuance and removal of employee, visitor and vendor identification badges, if utilized.
   - **c.** Upon arrival, photo identification shall be required for all non-employee visitors.

5. **Personnel Security and Verification:** Screen prospective employees consistent with local regulations. Verify employment application information prior to employment.

6. **Ocean Container and Truck Trailer Security:** Maintain container and trailer security to protect against the introduction of unauthorized material and/or persons into shipments. In the event containers are stuffed, inspections shall be made of all ocean containers or truck trailers prior to stuffing, including but not limited to the inspection of the reliability of the locking mechanisms of all doors.
   - **a.** **Ocean Container and Truck Trailer Seals:** Properly seal and secure shipping containers and trailers at the point of stuffing. Affix a high security seal to all access doors on truck trailers and ocean containers Such seals must meet or exceed the current PAS ISO 17712 standard for high security seals.
   - **b.** **Ocean Container and Truck Trailer Storage:** Empty or stuffed ocean containers and truck trailers must be stored in a secure area to prevent unauthorized access and/or manipulation.

7. **Information Technology (IT) Security**: maintain IT security measures to ensure all automated systems are protected from unauthorized access.
   - **a.** Use individually assigned accounts that require a periodic change of password for all automated systems.
   - **b.** Maintain a system to identify the abuse of IT resources including but not limited to improper access, tampering or altering of business data and will discipline violators.

8. **Procedural Security**: maintain, document, implement and communicate the following security procedures to ensure the security measures in this clause are followed and must include:

**a.** Procedures for the issuance, removal and changing of access devices.
**b.** Procedures to identify and challenge unauthorized or unidentified persons
**c.** Procedures to remove identification, facility, and system access for terminated employees.
**d.** Procedures for IT security and standards.
**e.** Procedures to verify application information for potential employees.
**f.** Procedures for employees to report security incidents and/or suspicious behavior.
**g.** Procedures for the inspection of ocean containers or truck trailers prior to stuffing.
**h.** Procedures to control, manage and record the issuance and use of high security bolt seals for ocean containers and truck trailers. Such procedures must stipulate how seals are to be controlled and affixed to loaded containers and shall include procedures for recognizing and reporting compromised seals or containers to Customs or the appropriate authority and (your company).

**9.** **Security Awareness Program:** A Security Awareness Program will be implemented by Service Provider and provided to its employees including awareness and understanding of the supply chain security program, recognizing internal conspiracies, maintaining cargo integrity, and determining and addressing unauthorized access. The Security Awareness Program should encourage active employee participation in security controls. Service Provider shall ensure that key personnel receive regular training which shall be no less than once per year on security procedures and requirements. Service Provider shall submit evidence of such Security Awareness training upon request.

**E.** **Questionnaire:** Service Provider will, upon request, complete a Supply Chain Security Questionnaires provided to Service Provider by (your company).

**F.** **Detailed Mapping**: Service Provider will, upon request, promptly provide a detailed mapping for planned routings and any Subcontractors involved in the transport of (your company) shipments.

**G.** **Site Visits:** Service Provider and its subcontractors shall be subject to periodic site visits during normal operating hours to confirm compliance with supply chain security standards.

**H.** **Breach of Security:** Service Provider and its subcontractors shall immediately notify (your company) of any actual or suspected breach of security involving (your company) cargo. This may include cargo theft, tampering, unauthorized access, or other activities that involve suspicious actions or circumstances related to (your company) cargo.

## *Appendix 5.3: Crisis-Management Program Core Elements Checklist*

| | |
|---|---|
| 1 | Has the organization designated one person as the company crisis leader? |
| 2 | If your organization includes more than one business entity, has a cross-business crisis management team been formed? |
| 3 | Does your crisis management team meet periodically to review roles and responsibilities and the effectiveness of crisis plans and procedures? |
| 4 | Does your crisis management team include representation from senior company leadership, human resources, legal, security, safety, communications, information technology and medical? (if such functions exist within your organization) |
| 5 | Does the organization have internal and external crisis communications plans for use during crisis situations? This plan should include one person designated as the company spokesperson regardless of number of sites impacted and business units impacted. |
| 6 | Has the crisis management communications leader been trained in communicating with internal and external stakeholders in time of crisis? |
| 7 | Are all crisis team leaders trained in roles and responsibilities, crisis plans and procedures and communications protocol? |
| 8 | Does your crisis management team maintain an up-to-date listing of all business sites, addresses, primary points of contact (including after hours contact information)? |
| 9 | Does your organization have a designated crisis management command center to assemble team members during a crisis situation? |
| 10 | Does your organization have a designated alternative crisis management command center in the event the primary site is unsuitable? |
| 11 | Are the primary and alternate crisis management command centers equipped and been operationally and routinely tested? |
| 12 | Does your organization have a designated crisis management leader at all business sites and in all critical functional area (I.e., supply chain, legal, human resources, etc.)? |
| 13 | Does your organization have a defined emergency notification communications system (manual or automated) to facilitate communication with employees during a crisis situation? |
| 14 | Does your organization test the emergency notification communication system periodically, but no less than annually? |
| 15 | Does the organization have a written crisis management plan including roles and responsibilities, crisis management procedures and communications protocols? |
| 16 | Does the organization have a documented and communicated procedure for employees to report incidents and events to the crisis team 24 hours a day? |
| 17 | Does your organization test the crisis management plan periodically at the business leadership level and all business sites, but no less than annually? |
| 18 | Does the organization include the crisis management program, emergency notification communications system and incident and event reporting in new employee orientation? |

## *Appendix 5.4: Sample Site Crisis Plan*

# Site Crisis Plan

**Document History**

| Version | Date (YYYY/MM/DD) | Name | Description |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**Questions**

Any questions regarding the content or the distribution list for this document should be directed to:

**Proprietary Information**

The information contained in this document is the sole property of COMPANY and its subsidiaries. Except as specifically authorized in writing by an authorized signatory of COMPANY, the recipient of this document shall keep all information contained herein confidential and shall protect the same, in whole or in part, from disclosure to third parties.

**PURPOSE**

The overall purpose of the workbook is to provide a consistent and complete Crisis Management Plan for the COMPANY **SITE** facility. This Plan builds upon the information contained in the COMPANY Crisis Manual and includes Business Continuity / Disaster Recovery Plans that are pertinent to each Business Site & Functional Unit located in this complex of facilities.

## 1. INTRODUCTION

A crisis is characterized as an extreme threat to important values, with intense time pressures, high stress, and the need for rapid but careful decision making. It is often a turning point in which a situation of impending danger to the organization runs the risk of escalating in intensity, interfering with normal business operations, jeopardizing the organization's public image, and damaging the bottom line. Either a sudden event, or a long smoldering issue may trigger a crisis. It is essential that we maintain an established and validated process to manage any conceptualized crisis, so as to limit the intensity of a negative threat or event to COMPANY' employees, products, services, financial condition and reputation.

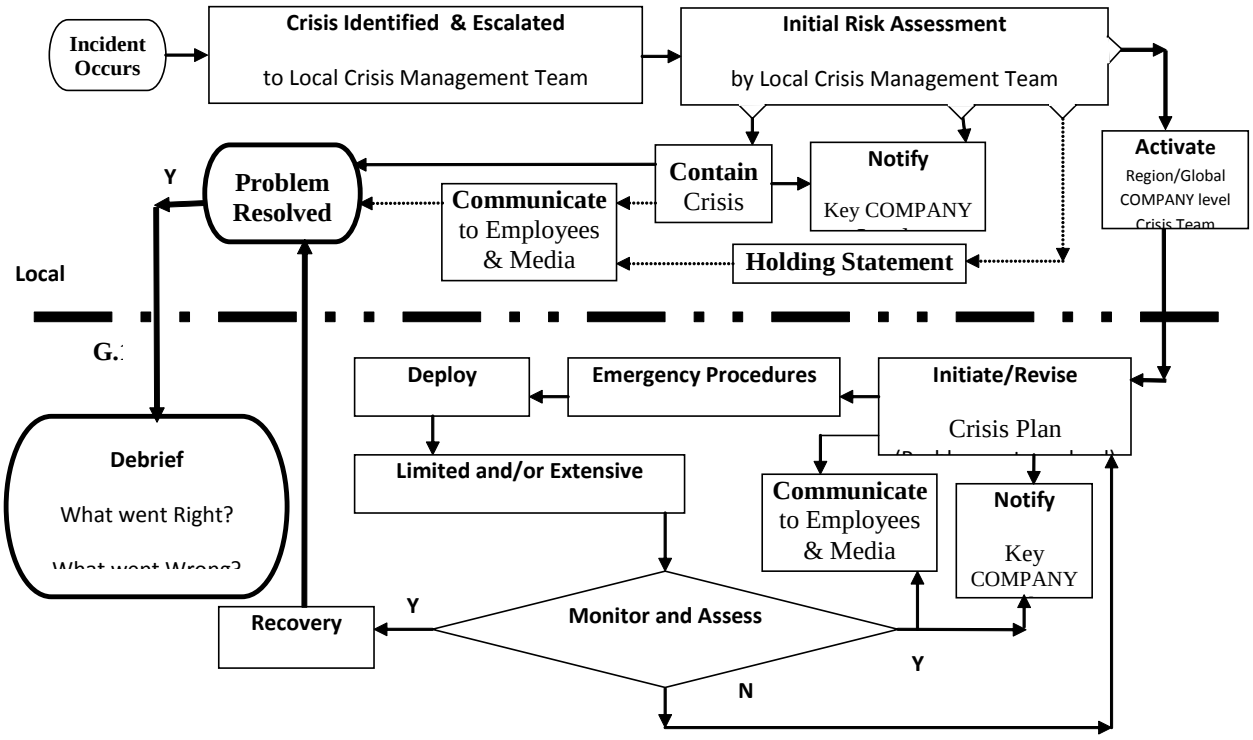
The **SITE** facility will first attempt to contain and manage crises on a local basis, escalating in accordance with the COMPANY'S Crisis Manual.

## 2. ROLES, RESPONSIBILITIES AND CONTACTS

**SITE** facility local crisis contacts are provided in Appendix A.

## 3. PROCESS

**SITE** will follow the crisis processes outlined below. Appropriate phases are linked to FirstAlert.



Below is a list of Crisis Management tools and templates. The described templates can be viewed and downloaded from the SCRLC web site (click here).

**Worksheet 1: Roles and Contact Information**

Identify the critical roles and personnel to be on call. Below you'll find a description of the roles and responsibilities that each Title may function within.

| Title | Roles And Responsibilities |
|---|---|
| Business/Modality Leader | • Lead the Individual Business Process Recovery Team which is responsible for ensuring the rapid recovery of business functions for their particular area in the event of a business interruption or disaster |
| Communications Manager /Spokesperson | • Provide ALL Communications Liaisons with Press<br>• Coordinate with Marketing for Customer Communications<br>• Lead the Public Relations Team which is responsible for serving as the sole source for dissemination of information related to the disaster to the public, including news media |
| Crisis Management Leader | • Mobilize and Lead Crisis Response Team<br>• Authorize Move to Crisis Command Center<br>• Co-ordinate All Departments<br>• Gather Facts<br>• Inform COMPANY President & CEO |
| EHS Manager | • Ensure Employee and On-Site Personnel Safety<br>• Ensure Health and Safety Requirements are Met<br>• Communicate Status with the Crisis Management Leader |
| Facilities Manager | • Assess Security / Secure the Physical Environment<br>• Communications Liaison with Emergency Services<br>• Locate Alternative Facilities (as appropriate)<br>• Ensure Open Emergency Exit Passage Ways<br>• Communicate Status with the Crisis Management Leader<br>• Lead Facilities Assessment Team which:<br>o Conducts initial assessment of facilities damage<br>o Provides support to evacuated employees<br>• Lead the Site Evaluation and Restoration Team which:<br>o Assesses the impact of the disaster<br>o Gathers information regarding the restoration of damaged facilities |
| Finance | • Provide Authorization for Emergency Purchases<br>• Lead the Accounting Recovery Team which manages monetary needs associated with recovery operations<br>• Lead the Travel and Lodging Recovery Team which is responsible for arranging all travel and lodging requirements for the recovery operations |
| Human Resources (HR) | • Ensure Health and Safety Requirements are Met<br>• Work with Communications Manager to Provide All Emergency |

| | |
|---|---|
| | Employee Communications<br>• Lead the Human Resources Recovery Team which provides support to personnel issues that are critical to controlling the recovery effort |
| IM Applications Support Manager | • Activate IM Applications |
| IM Infrastructure Support Manager | • Reinstate IM Infrastructure<br>• Reinstate Databases<br>• Redirect Telephone Lines<br>• Install PC's and Telephony at Crisis Command Center<br>• Communicate Status with the IM Leader<br>• Lead Information Management (IM) Recovery Team, which is responsible for the recovery of telecommunications, and key IT systems at the recovery location. |
| IM Leader | • Ensure appropriate IM Staff Assigned<br>• Restore Mission Critical IM Systems<br>• Implementation of Crisis Command Center<br>• Secure the Systems Environment<br>• Communicate Status with the Crisis Management Leader |
| Legal Manager | • Provide Legal Guidance Regarding Crisis to Crisis Management Leader and to COMPANY President & CEO<br>• Lead the Risk Management Recovery Team, which is responsible for the coordination of legal and insurance issues related to business interruption. |
| Marketing | • In conjunction with the Communications Manager, develop customer-oriented communications |
| Sales / Service | • Communicate ONLY HQ-Authorized communications to customers<br>• Reassure Customers of Proven Effectiveness of COMPANY Business Continuity Plans |
| Security Manager | • Ensure Protection of Facilities and Employees<br>• Liaise with Law Enforcement Agencies |
| Sourcing Manager | • Ensure Viability of Supply Chain |
| V.P. Operations | • Initiate Recovery Plans for Mission Critical Processes<br>• Assemble Team for Long Term Recovery Strategy<br>• Communicate Status to Crisis Management Leader |

**Worksheet 2: Distribution and Procedure List**

Create a Distribution List in your company address book of the critical roles and personnel identified in Section 1.

Create a list of COMPANY policies, procedures and training so that the team can follow company standards in handling issues during the Crisis Management phase. Some of these include:

- Crisis Management Policy

- Company Global Security Policy
- Website
- Workplace Violence Guidelines
- Crisis Management Training

**Worksheet 3: Initial Assessment Checklist**

An Initial Assessment checklist enables the crisis response team to capture the facts of the incident at a high level. Assigning a Case Number allows the team to collate other tools and templates to the same case.

**Worksheet 4: Extent of Damage Report**

An Extent of Damage Report can be used during the initial analysis as well as later during the most in depth review. Using the report at multiple points in the Crisis Management process enables the team to assess how well the initial and on-going assessments were captured.

**Worksheet 5: Site Damage Evaluation**

A Site Damage Evaluation goes into more depth than an Extent of Damage Report and can be used for each item captured on the Extent of Damage Report.

**Worksheet 6: Site Security**

A Site Security report is an assessment tool to determine if security gaps exist as a result of the incident.

**Worksheet 7: Crisis Management Team Task Checklist**

A Crisis Management Team Task Checklist is a tool for the team to use to identify if specific tasks have been completed, by whom, and when.

**Worksheet 8: Critical Process Checklist**

A Critical Process Checklist allows the team to assess which critical processes have or will be impacted by the incident.

**Worksheet 9: Business Critical Telephone Numbers**

A Business Critical Telephone Number list allows the team to have easy access to corporate profile information for services (e.g. healthcare, software support, etc.)

**Worksheet 10: Business Crisis Management Team**

A Business Crisis Management Team worksheet identifies they key information for enterprise level leadership who need to be kept apprised of the situation.

**Worksheet 11: Crisis Response Damage and Assessment**

A Crisis Response Damage Assessment worksheet extends the Business Crisis Management Team beyond enterprise level executives to individuals responsible for business services (e.g. communications, security, legal, etc.).

**Worksheet 12: Subject Matter Experts**

A Subject Matter Expert report identifies who the expert is for a business process.

**Worksheet 13: Business Crisis Management Assessment, Recovery, and Subject Matter Experts**

A Business Crisis Management Assessment, Recovery, and Subject Matter Experts worksheet identifies the roles, responsibility and authority to handle the incident.

**Worksheet 14: External Agencies and Action Contacts**

An External Agency and Action Contacts matrix provides the team with a ready list of local and federal services which may needed to support the incident.

**Worksheet 15: Network Connectivity**

A Network Connectivity report identifies the organizational networks which may be called upon for support.

**Worksheet 16: Post Office and Courier Recovery**

A Post Office and Courier Recovery report identifies the key services which may be utilized to help expedite processing of crisis response actions.

**Worksheet 17: Business Critical Suppliers**

A Business Critical Supplier report identifies suppliers, service provider, and government agencies which may need to be made aware of the incident.

**Worksheet 18: Software Vendors**

A Software Vendor report tracks the owner and contact information for software applications which may be vulnerable due to the incident.

**Worksheet 19: Supplier Communications**

A Supplier Communication report can help a team track which suppliers have received communications and which communications they have received.

**Worksheet 20: IT Team**

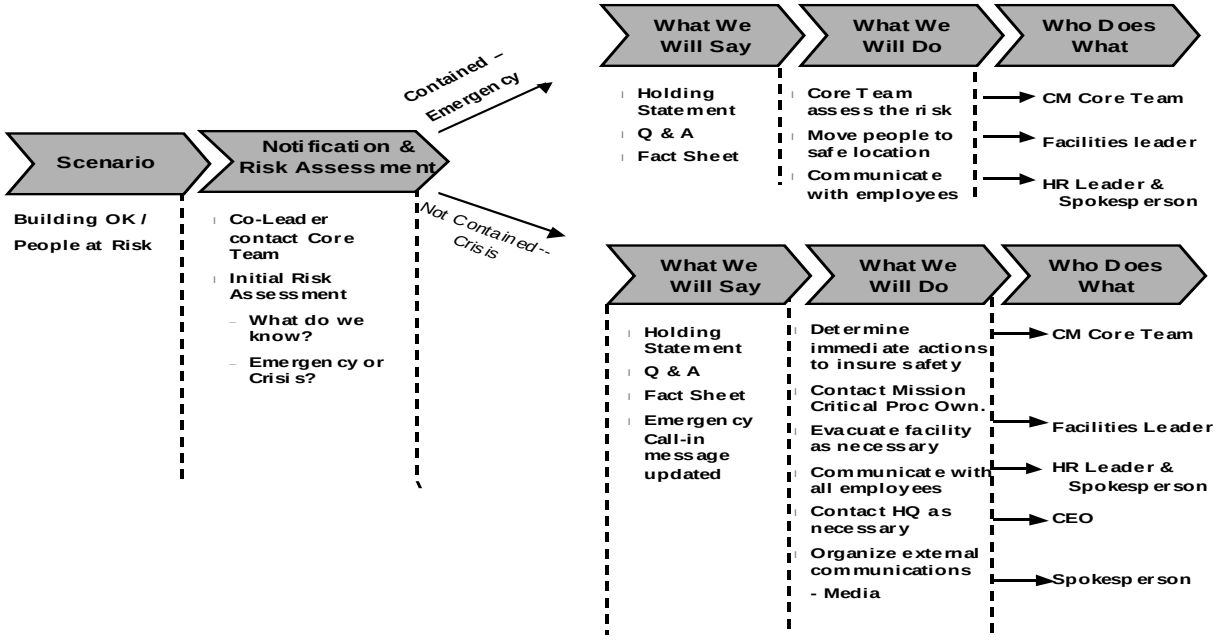
An IT Team report identifies the critical Subject Matter Experts needed to repair or rebuild systems.

**Worksheet 21: External Agencies**

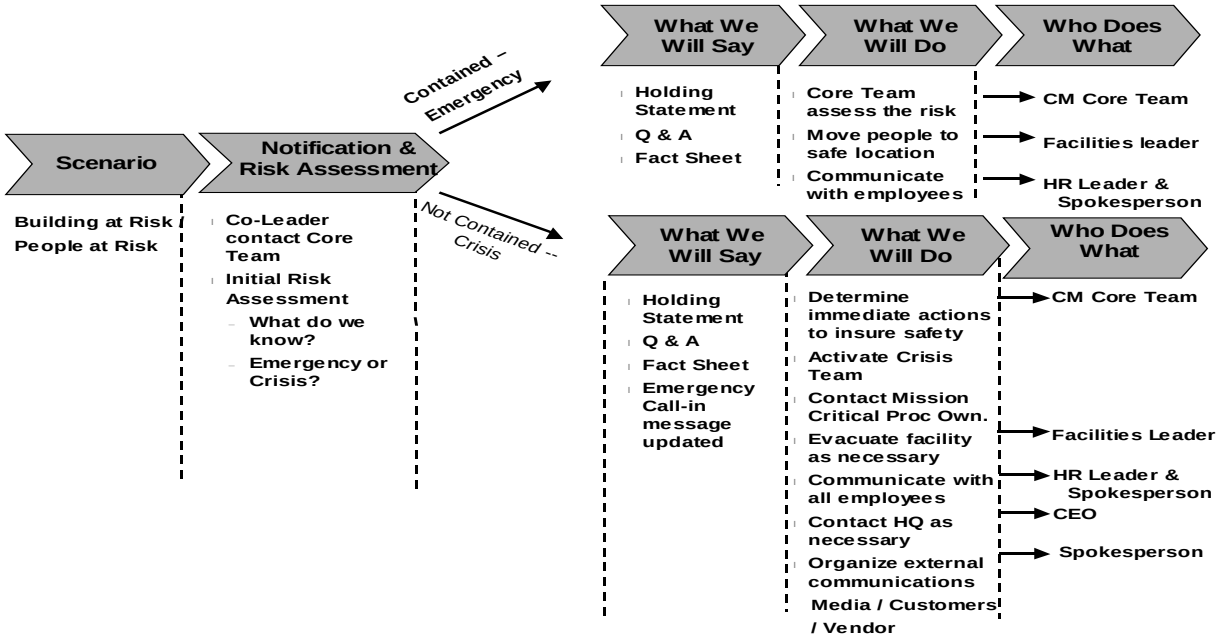
An External Agency report identifies the external agencies which may need to be made aware of the situation (e.g. radio, television, newspaper, etc.).

**The following diagrams identify process flows to guide a Crisis Management team in managing incident response.**

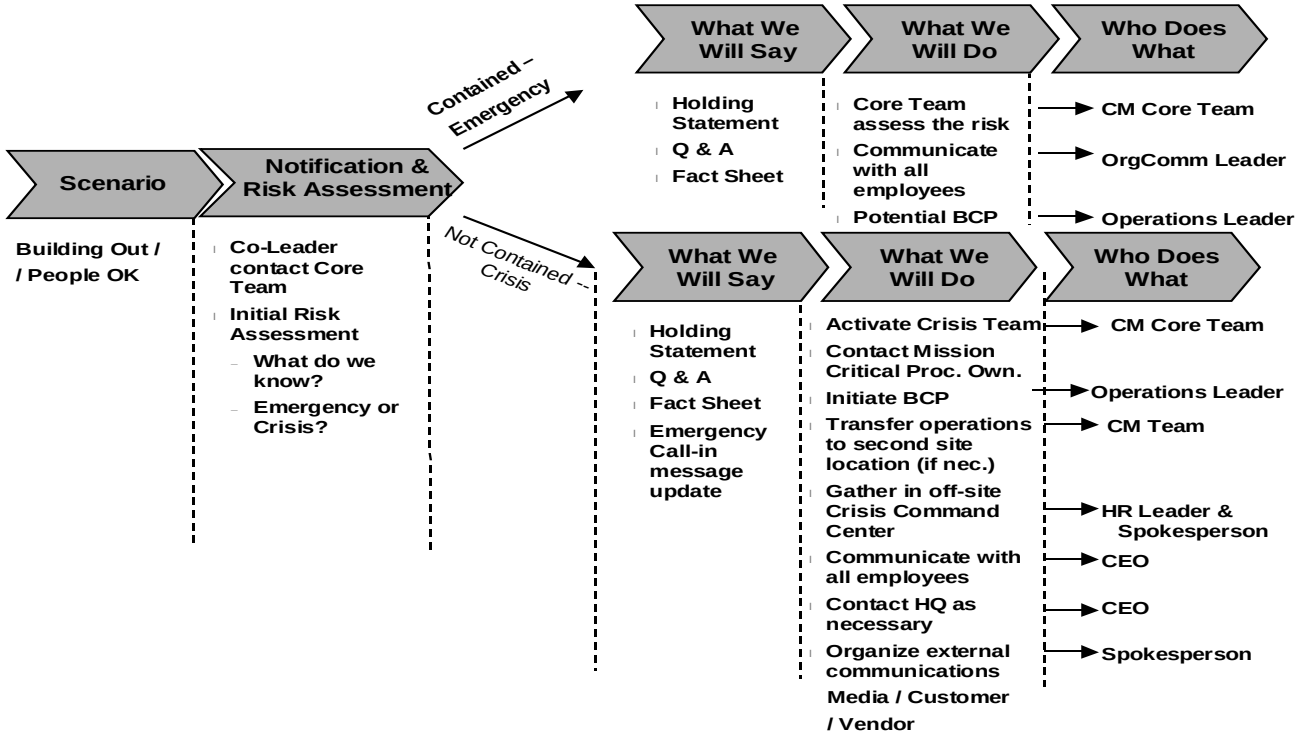
**Crisis Management Diagram 1:** ***Building OK / People At Risk***



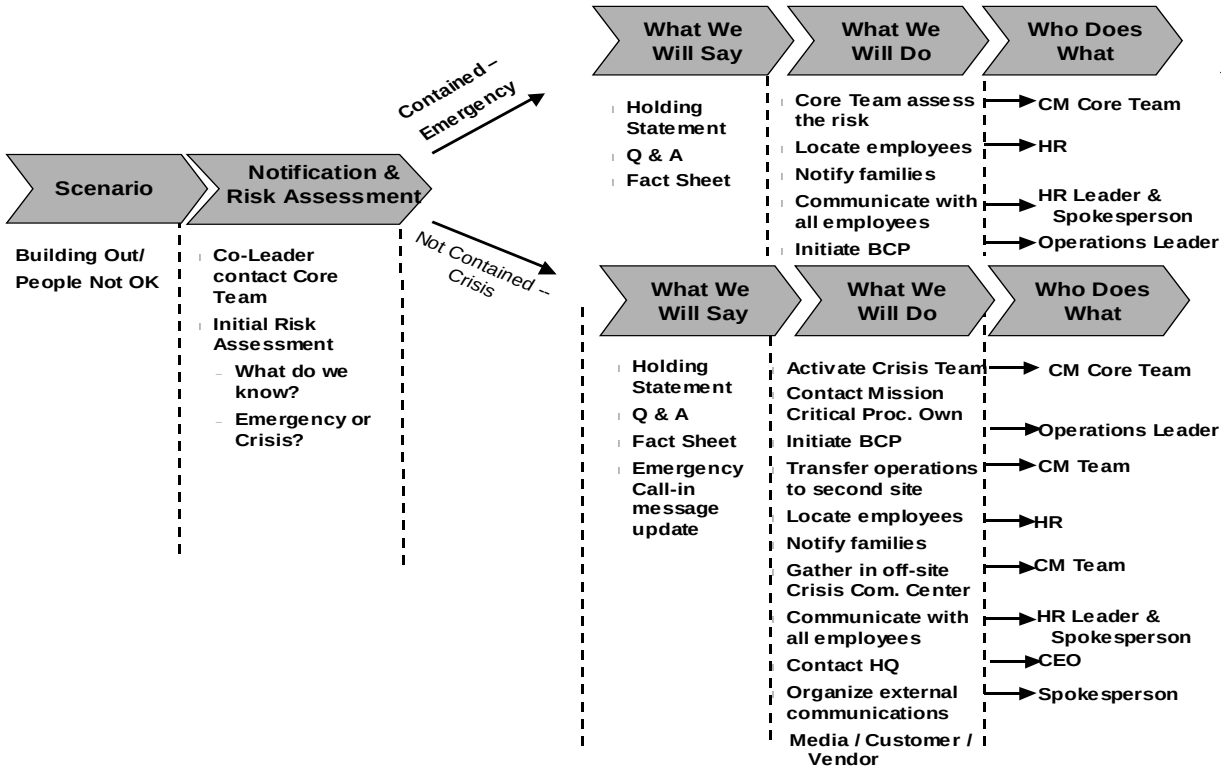

**Crisis Management Diagram 2:** ***Building At Risk / People At Risk***



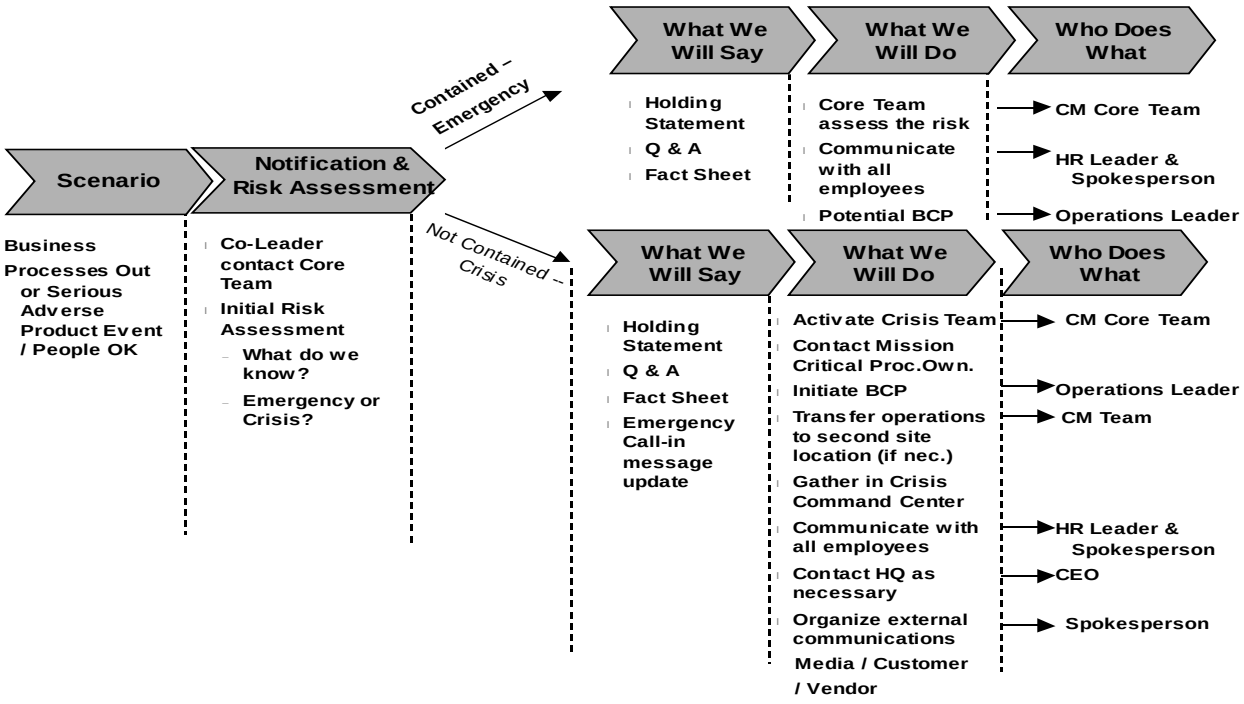
**Crisis Management Diagram 3: *Building Out / People OK***




**Crisis Management Diagram 4: Building Out / People Not OK**



***Crisis Management Diagram 5: Business Processes Out or Serious Adverse Product Event / People OK***

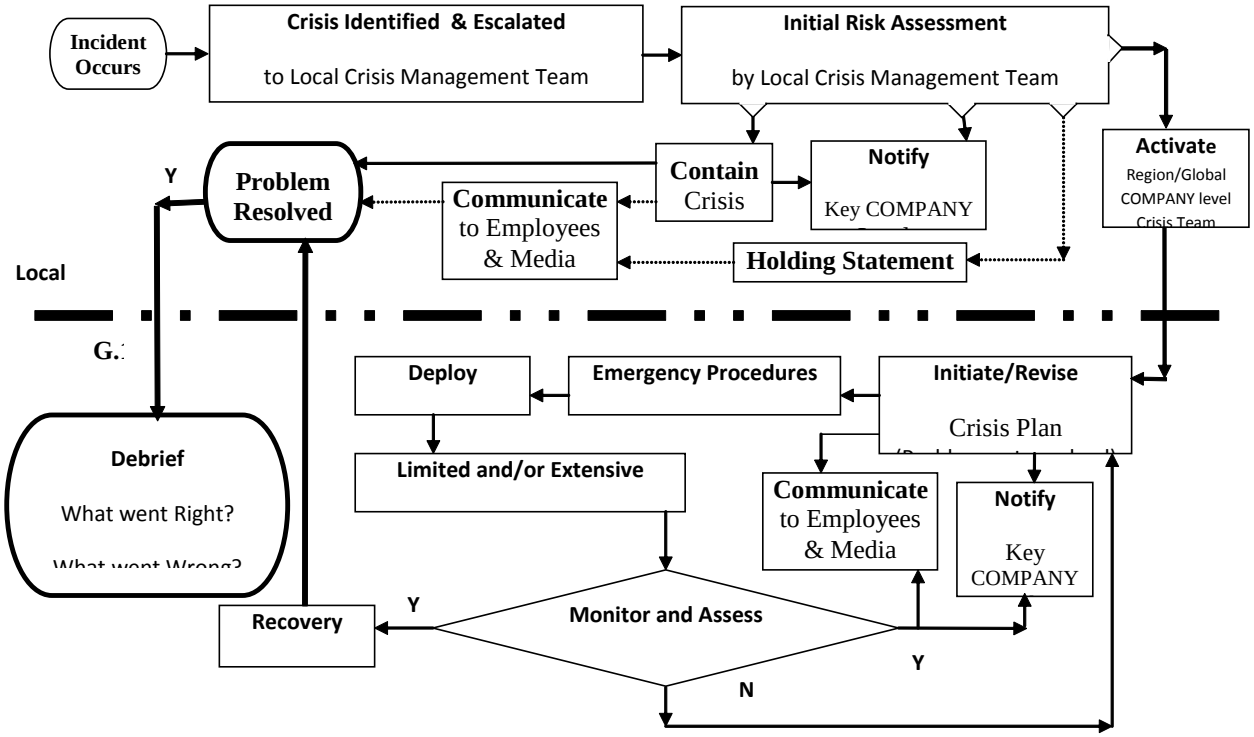


# CRISIS COMMUNICATIONS PLAN

## Crisis Calls

In all crisis situations, the site Crisis Team Leader should alert the appropriate COMPANY Pole Crisis Leader listed in §E2.2. The company Spokesperson is given in §E2.2 and §E2.4.

Follow the steps in the Crisis Process Map below:



## SUMMARY of SITE REQUIREMENTS

**SITE Facility Passport**

(Fire, Severe Weather, Medical Emergency, Hazardous Spills)

**Site Facility Passport**

**Emergencies Call**
**XXX-XXX-XXXX**

Fire
Severe Weather
Medical Emergency
Hazardous Spills

**All calls will be answered by the guard at the Main Guardhouse. You will need to provide the following information :**

1) **YOUR NAME**
2) **TYPE OF EMERGENCY (FIRE, MEDICAL, SPILL, ETC.)**
3) **YOUR LOCATION (Building, Floor & Column Number)**

**REMEMBER… REMAIN CALM& STAY ON THE PHONE!!**

**The guard will notify the appropriate emergency response personnel.**

**What to do when an alarm sounds:**

Wait for INSTRUCTIONS over the PA system such as:
- Activate Response Team (medical, fire, spill, etc.)
- Proceed to Severe Weather Shelter Area (tornado, severe weather, etc.).
- Building evacuation (fire, hazardous spills, etc.)

COMPLY with instructions CALMLY & QUICKLY.

**Facility Rules for Visitors/Vendors**

- Posted speed limits must be observed.
- Wearing of safety glasses and protective footwear are required at all times in designated areas.
- Smoking is allowed in designated areas outside of the facility only.
- Cameras are prohibited on COMPANY premises without prior approval of the security department.
- All on-site injuries, no matter how slight, must be reported. Medical facilities are available on site.
- If medical assistance is required, notify your COMPANY contact person or dial NNNNN from any phone.
- In the event of a facility evacuation, all visitors/vendors are to use any external door convenient to your location (See map on inside of passport).
- In the event of a severe weather emergency, proceed to the nearest shelter area. (See map on inside of passport and maps posted throughout the facility for severe weather shelter areas.)
- Pedestrians on the shop floor must ALWAYS be aware of motorized equipment such as forklifts and hand trucks.
- All chemicals brought into the facility must have prior site approval. Contact the COMPANY person in advance with a Material Safety Data Sheet.
- The rules and regulations contained in this booklet are general and subject to change Specific safety rules, regulations and procedures will be brought to your attention as the need arises.
- COMPANY insist on full cooperation and observance of all safety rules and regulations. Everyone will benefit from good safety practices.

**Emergency Maps**

# FACILITY EMERGENCY MAP SHOWING LOCATIONS OF CRISIS ROOMS

# FLOOR 1

# FACILITY EMERGENCY MAP SHOWING LOCATIONS OF CRISIS ROOMS

# FLOOR 2

## Crisis Command Center – COMPANY CRISIS ROOM

**COMPANY SITE has designated XXXXX as its Crisis Room.**

Should the Primary Crisis Room for any reason be inaccessible (power failure, physical damage, etc.), the **Secondary is pre-designated as the alternate Crisis Room**. The room and all of its equipment are configured so that it can become fully operational at any time 24/7. Provisions are in place to supply ventilation, power and computer network access 24/7.

**Primary and Secondary locations** are used as regular conference rooms, to maximize the cost efficiency of the space. Because a crisis could occur at any time and because the primary purpose of the room is for crisis purposes, all staff booking the room should understand they could be pre-empted at any time and on very short notice.

NOTE: All crisis-related equipment (phones, display walls, other equipment) is secured and designed so that all of this equipment can be unlocked, put in place and activated as quickly as possible.

The general parameters for the equipment in the Crisis Room are:

- Laptop port with full access to COMPANY network at each seat
- Multi-directional speakerphone in the ceiling
- Electronic display wall which includes facilities for video playback or broadcast monitoring; maps; crisis log; PowerPoint; technical diagrams; videoconferencing; etc.
- Easels with flip charts; or chalk board with print capability

and Proximity to:

- Fax machine
- Copier
- Printer
- Facilities for refreshments

In the case of a crisis, the room should be staffed with at least 2 to 3 support personnel to handle phone calls, copying and fax and IT support. The maintenance and activation protocol is established along the following guidelines:

- Generally, Facilities management personnel has responsibility for activation
- Periodic walk-through of the room is performed to be certain that all facilities are intact and operable.

**Business Unit Plans**

- **Communications Plan**
  - o
- **Information Management Plan:**
  - o
- **Facility Plan:**
  - o
- **Site Name Site Security Manual**
  - o
- **Human Resources Plan:**
  - o
- **Supply Chain Plan:**
  - o
- **Security Requirements Plan:**

  **If this is a multi-tenant site, the site is managed by XXXXX. XXXXX are employed by the YYYYY through their Agent ZZZZZ. The reporting lines are that XXXXX will contact their own Management & YYYYY first with tenants notified immediately afterwards.**

  **XXXXX Tel. No.**

  **The security response procedure is provided to the security guard though their assignment instructions:**
  - **If security sounds an alarm, police are automatically informed**
  - **If situation escalates, contact Facilities and Security managers – AAAAA&BBBBB**

  **IM Contact currently assigned – CCCCC**

- **Medical Response Plan**

**COMPANY Medical Emergency Response:**
**Chemical, Biological, Radiological, Nuclear and Environmental (CBRNE)**

**Medical Response: EVENT DESCRIPTION**

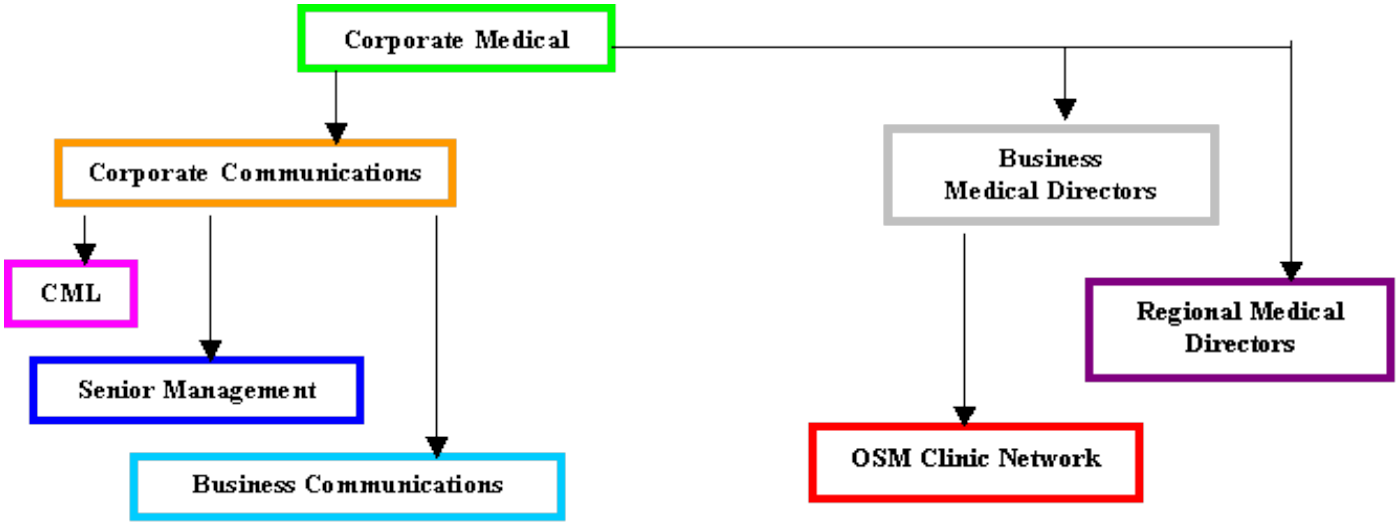
**Preparedness and Prevention:**

**Detection and Surveillance:**

**Diagnosis and Characterization of Biological and Chemical Agents:**

**Response:**

**Communication Systems:**




**Below are the options for the local site for communication and information dissemination.**

**Telephone:** will be primary with teleconference for company meetings

**Web:** Instant Messaging Service, Web Meeting, in COMPANY and web page information in addition to local radio.

**Local radio net (hand held):** will be used for emergency and urgent communications with response teams (medical, spill, fire, security).

**Cell phones:** Will be used for both emergency communications as well as more routine communications. This may become primary with a local telephone system failure.

**Runners:** With local failures of multiple communications systems "runners" may become necessary to keep command and control of resources.

**Other:** Access to other systems including community radios (fire/police), Federal radio (National Guard), HAM radio, etc. may vary widely and be unavailable.

External communications will be carefully channelled through the CML team communications team. Medical staff will not directly communicate with press or external community organizations without the knowledge and approval of the CML communications team. This is a critical element of the response plan to assure that all communications are accurate, coordinated and timely.

## Community Partnerships and Contacts:

- ***State Homeland Defense Council:***
- ***State Division of Public Health:***
- ***State Laboratories:***
- ***Regional Department of Public Health***
- ***County Department of Public Health:***
- ***SITE County Department of Public Health***
- **State and Federal Resources**
- ***State Public Health Departments***
- ***State Domestic Preparedness***
- ***Poison Control Centers***
    - State: toll-free telephone
    - National: toll-free telephone 1-800-222-1222
- ***City Health Dept.***
- ***State Laboratory***
- ***US Homeland Security***
  **http://www.ready.gov/**
- ***Center for Disease Control (CDC)***
  **http://www.cdc.gov/**
- ***Agency for Toxic Substances and Disease Registry (ATSDR)***
  **http://www.atsdr.cdc.gov/**
- ***Index of FEMA Web Site***
  **http://www.fema.gov/fema**
- ***Homeland Defense***
  **http://hld.sbccom.army.mil/**
- ***SITE County Sheriff***

**Crisis Emergency Phone Line**

- **Toll Free (US)**
- **From Outside (US)**
  **Passcode:**

# Facility Crisis Communications Information

**Date_____**

**I Facility/Location_____**

First Response Call_____

On-site EHS/phone/Email_____

On-site Security Lead/phone/Email_____

Plant Manager/phone/Email_____

EAP Contact/phone/Email_____

On-site Communications Contact/phone/Email_____

Companies with Contractors on site/Phone_____

_____

Is there a facility emergency response plan?_____ Where?_____

**II Business Contacts**

Business Medical Director/phone/Email_____

Backup Medical Lead/phone/Email_____

Business Security Lead/phone/Email_____

Business EHS Lead/phone/Email_____

Business EAP contact/phone/Email_____

Business Communications contact/phone/Email_____

**III Corporate Contacts**

**IV Site Community Contacts**

EMS contact_____

Phone_____

Local Public Health contact_____

Phone_____

Local Hospital Name_____

ER Contact/phone_____

Local Pharmacy/Phone_____

**State Health Department Phone_____**

**State Health Department**

**Email_____**

**CDC Emergency Preparedness & Response Branch 1-770-488-7100**

**CDC Health Emergency and Preparedness Web Site**

**http://www.bt.cdc.gov**

## *Appendix 6.1: Sample Regulatory Impact Assessment*

An organization may use a Regulatory Impact Assessment tool to map existing regulatory requirements and what portion of the supply chain it affects as well as identify where new regulations affect your supply chain.

The table below shows where a regulatory/compliance requirement impacts the supply chain.

| Reulatory / Compliance Requirement | Cargo Supply Chain<br>Indicate with an "X" where the requirement affects the supply chain. | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Originating Named Place | Customs Clearance (Export) | Loading | Inland Freight | Carrier Not Unloaded | Alongside ship Port of Loading | On-Board vessel Port of Loading | Ocean/Air Freight | On-Board vessel Port of Destination | Unloaded Port of Destination | Customs Clearance (Import) | Inland Freight | Named Destination |
| Supply Chain Security program | x | x | x | x | x | x | x | x | x | x | x | x | x |
| Cargo Screening / Scanning | | | | | | x | x | x | | | | | |
| Advanced Data Requirements | x | | | | | x | x | x | | | | | |
| High security bolt seals (on int'l incoming truck and ocean containers | x | | x | x | x | x | x | x | x | x | x | | |


| Reulatory / Compliance Requirement | Cargo Supply Chain<br>Indicate with an "X" where the requirement affects the supply chain. | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Originating Named Place | Customs Clearance (Export) | Loading | Inland Freight | Carrier Not Unloaded | Alongside ship Port of Loading | On-Board vessel Port of Loading | Ocean/Air Freight | On-Board vessel Port of Destination | Unloaded Port of Destination | Customs Clearance (Import) | Inland Freight | Named Destination |
| Supply Chain Security program | x | x | x | x | x | x | x | x | x | x | x | x | x |
| Cargo Screening / Scanning | | | | | | x | x | x | | | | | |
| Advanced Data Requirements | x | | | | | x | x | x | | | | | |
| High security bolt seals (on int'l incoming truck and ocean containers | x | | x | x | x | x | x | x | x | x | x | | |


| | |
|---|---|
| Red | Have no controls or visibility |
| Yellow | Some controls and/or visibility |
| Green | Have controls and visibility |

You may then want to identify which organization is impacted and needs to address such requirements.

| Reulatory / Compliance Requirement | Responsible Organization | | | | | |
|---|---|---|---|---|---|---|
| | Supply Chain Security | Supply Chain Logistics | Import Export Operations | Supplier Management | Contracts | Government Affairs |
| Supply Chain Security program | x | | | | x | |
| Cargo Screening / Scanning | | x | | x | | x |
| Advanced Data Requirements | | | x | | x | |
| High security bolt seals (on int'l incoming truck and ocean containers | x | | | | | |


| Reulatory / Compliance Requirement | Responsible Organization | | | | | |
|---|---|---|---|---|---|---|
| | Supply Chain Security | Supply Chain Logistics | Import Export Operations | Supplier Management | Contracts | Government Affairs |
| Supply Chain Security program | x | | | | x | |
| Cargo Screening / Scanning | | x | | x | | x |
| Advanced Data Requirements | | | x | | x | |
| High security bolt seals (on int'l incoming truck and ocean containers | x | | | | | |

# Bibliography

## *Cited in Text*

ASIS International, "Organizational Resilience: Security, Preparedness, and Continuity Management Systems — Requirements with Guidance for Use," Business Continuity Management Systems: Requirements with Guidance for Use, ASIS SPC.1-2009, November 2, 2010.

ASIS International and British Standards Institution (BSI), "Business Continuity Management Systems: Requirements with Guidance for Use," ASIS/BSI BCM.01-2010, November 2, 2010.

British Standards Institute, "Risk Management: Code of Practice," BS 31100, October 2008

Hepenstal, Ann, and Boon Campbell, "Maturation of Business Continuity Practice in the Intel Supply Chain," *Intel Technology Journal*, Vol. 11, Issue 2, May 2007, pp. 165-171. As of May 29, 2011: http://www.intel.com/technology/itj/2007/v11i2/8-business-continuity/1-abstract.htm.

International Organization for Standardization, "Specification for Security Management Systems for the Supply Chain," ISO 28000, 2007.

International Organization for Standardization, "Risk Management — Principles and Guidelines," ISO 28000, 2009.

International Organization for Standardization, "Risk Management—Risk Assessment Techniques," ISO 31010, 2009.

International Organization for Standardization, "Freight Containers—Mechanical Seals," ISO 17712, 2010.

Lee, Don, and David Pierson, "Disaster in Japan Exposes Supply Chain Flaw," Los Angeles *Times*, April 6, 2011. As of May 28, 2011: http://articles.latimes.com/2011/apr/06/business/la-fi-quake-supply-chain-20110406.

Moore, Nancy Y., Clifford A. Grammich, and Robert Bickel, *Developing Tailored Supply Strategies*, Santa Monica, Calif.: RAND Corporation, 2007. As of May 22, 2011: http://www.rand.org/pubs/monographs/MG572.html.

Zsidisin, George A., Gary L. Ragatz, and Steven A. Melnyk, "Effective Practices for Business Continuity Planning in Purchasing and Supply Management," East Lansing, Mich.: Michigan State University, July 21, 2003.

## *Other Relevant Publications*


Berman, Al, "Business Continuity in a Sarbanes-Oxley World," *Disaster Recovery* Journal, Vol. 17, No. 2, Spring 2004, pp. 18-24.

Castillo, Carolyn, "Disaster Preparedness and Business Continuity Planning at Boeing: An Integrated Model," *Journal of Facilities Management*, Vol. 3, No. 1, July 2004, pp. 5-26.

Chopra, Sunil, and ManMohan S. Sodhi, "Managing Risk to Avoid Supply-Chain Breakdown," *MITSloan Management Review*, Vol 46, No. 1, Fall 2004, pp. 53-61. As of August 6, 2011: http://sloanreview.mit.edu/the-magazine/2004-fall/46109/managing-risk-to-avoid-supplychain-breakdown/.

Christopher, Martin, "Understanding Supply Chain Risk: A Self-Assessment Workbook," Cranfield University, School of Management, Department for Transport, 2003. As of August 10, 2011: https://dspace.lib.cranfield.ac.uk/bitstream/1826/4373/1/Understanding_supply_chain_risk.pdf.

Ellis, Simon, "Supply Chain Risk Management: A Best Practice Case Study of Cisco," *Manufacturing Insights*, June, 2009.

Favre, Donovan, and John McCreery, "Coming to Grips with Supplier Risk," *Supply Chain Management Review*, September 1, 2008.

Finch, Peter, "Supply Chain Risk Management," *Supply Chain Management: An International Journal*, Vol. 9, No. 2, 2004, pp. 183-196.

Giunipero, Larry C., and Reham Aly Eltantawy, "Securing the Upstream Supply Chain: A Risk Management Approach," *International Journal of Physical Distribution & Logistics Management*, Vol. 34, No. 9, 2004, pp. 698-713.

Hillman, Mark, and Heather Keltz, "Managing Risk in the Supply Chain – A Quantitative Study," AMR Research, 2007.

Norrman, Andreas, and Ulf Jansson, "Ericsson's Proactive Supply Chain Risk Management Approach After a Serious Sub-supplier Accident," *International Journal of Physical Distribution and Logistics Management*, Vol. 34, No. 5, 2004, pp. 434-456.

Pitt, Michael, and Sonia Goyal, "Business Continuity Planning as a Facilities Management Tool," *Facilities*, Vol. 22, No. 3/4, 2004, pp. 87-99.

Ritchie, Bob, and Clare Brindley, "Supply Chain Risk Management and Performance: A Guiding Framework for Future Development," *International Journal of Operations and Production Management*, Vol. 27, No. 3, 2007, pp. 303-322.

Sheffi, Yosef, *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage*, Cambridge, Mass.: MIT Press, 2005.

Sheffi, Yossi, and James B. Rice Jr., "A Supply Chain View of the Resilient Enterprise," *MITSloan Management Review*, Vol. 47, No. 1, Fall 2005, pp. 41-48. As of August 6, 2011: http://sloanreview.mit.edu/the-magazine/2005-fall/47110/a-supply-chain-view-of-the-resilient-enterprise/.

Smith, Briony, "Intel: Disasters Can Be 'Business As Usual' With Enough Planning," *ComputerWorld*, June 18, 2008. As of August 11, 2011: http://www.computerworld.com/s/article/print/9100518/Intel_Disasters_can_be_business_as_usual_with_enough_planning?taxonomyName=Security&taxonomyId=17.

Solomon, Lance, and Joe McMorrow, "Case Study: Chengdu Earthquake Crisis Response," Supply Chain Risk Leadership Council Newsletter, Fourth Quarter, 2008. As of August 11, 2011: http://www.scrlc.com/newsletter-readMore.php?aID=134.

Verstraete, Christian, "Share and Share Alike," *Supply Chain Quarterly*, Quarter 2, 2008.

Zsidisin, George A., Alex Panelli, and Rebecca Upton, "Purchasing Organization Involvement in Risk Assessments, Contingency Plans, and Risk Management: An Exploratory Study," *Supply Chain Management*, Vol. 5, No. 4, 2000, 187-198.

Zsidisin, George A., "Business and Supply Chain Continuity," *Critical Issues Report*, January 2007.